A Risk Management Framework for Data Security and Privacy of Wireless Body Area Network based Healthcare Applications

This thesis is submitted

To

DCU

Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Under the delegation of authority from the
Higher Education and Training Award Council

For the award
Of
Doctorate of Philosophy
By

Pangkaj Chandra Paul

Prepared under the supervision of
Dr John Loane
Dr Gilbert Regan
Prof. Fergal McCaffery
School of Informatics and Creative Arts,
Dundalk Institute of Technology

May 2024

Declaration

We, the undersigned declare that this thesis entitled *'A Risk Management Framework for Data Security and Privacy Risk Management Framework of Wireless Body Area Network based Healthcare Applications'* is entirely the author's own work and has not been taken from the work of others, except as cited and acknowledged within the text.

The thesis has been prepared according to the regulations of Dundalk Institute of Technology and has not been submitted in whole or in part for an award in this or any other institution.

Author Name: ...Pangkaj Chandra Paul........................

Author Signature: ....

Date: .... 25-11-2022..

Supervisor Name: ...Dr John Loane...............................

Supervisor Signature: ... John Loane ....

Date: ....25-11-2022...

Acknowledgements

I am grateful to my supervisors, Dr John Loane, Dr Gilbert Regan and Prof Fergal McCaffery, who were the main sources of inspiration and motivation during the whole work of the thesis. Their valuable suggestions, encouragement, guidance, advice, and countless discussions during this thesis work were incomparable. Without their valuable time, this thesis would not have been feasible. Thank Arthur McMahon, Chief Technical Officer at STATSports Group Limited. I am also grateful to STATSports's development teams, who participated in this research work.

I would like to thank my parents, Hari Bhushan Paul and Laxmi Rani Paul, for all their support and encouragement throughout my studies. I would also like to thank my uncle Manik Paul. They have always emphasised the value of education, had faith in my ability, and encouraged me in whatever I wanted to accomplish. Thanks also to my sister Anamika Paul Tuli for her support and encouragement throughout the thesis work.

I am thankful to my colleagues at RSRC, especially, Surafel, Hamsini, and Ceara, for their support and precise time for endless discussion. I am also grateful to my friend Mohammad Abdur Razzak for his continuous motivation and guidance to overcome any problem. Finally, I would also like to thank all the participants who participated in this research and provided their invaluable feedback.

This research was supported with the financial support of the Science Foundation Ireland Grant No. 13/RC/2094_2 and cofounded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero. This research was partly supported by the HEA COVID-19 Relief Fund.

Abstract

Wireless Body Area Network (WBAN) based applications are gaining popularity due to recent advances in sensor technology, integrated circuits, mobile apps and wireless communication. The literature review conducted as part of this research indicates that the most challenging issues related to developing a WBAN based healthcare application are energy efficiency, antenna design, assuring quality of service, and security and privacy. WBAN applications operate in environments where people may have open internet access, making the application vulnerable and open to larger attack surfaces. Attacks can affect the performance and availability of the service, sometimes leading to life-threatening situations or even death.

Through the literature review and an interview with one WBAN development organisation, this research has identified that assuring security and privacy while collecting, transmitting, processing, and storing personal health record (PHR) data is a key challenge for developers. The reasons for this challenge include (i) developers have limited knowledge of market-specific regulatory requirements and standards, and (ii) there are a vast number of controls with insufficient implementation detail. The literature review also found no complete solution exists for assuring data security and privacy while also meeting the regulatory requirements for WBAN based healthcare applications.

To address these challenges for assuring security and privacy, this research has developed a data security and privacy risk management (WBANSecRM) framework that will assist the developer in assuring security and privacy of the data and put them on the path to regulatory compliance. The framework outlines the process to identify the list of assets, threats, and vulnerabilities specific to WBAN applications. The framework also consists of a comprehensive list of controls, along with implementation details to mitigate the threats and vulnerabilities. The framework has been validated by implementation in an organisation that develops WBAN applications and was further validated by expert review.

Glossary Of Terms

WBAN - Wireless Body Area Network

WSN - Wireless Sensor Networks

UWB - Ultra-wideband is a radio technology that can easily use a low energy level for short-range, high-bandwidth communications

QoS - Quality of Service

e-PHI - Electronic Protected Health Information is information that is produced, saved, transferred, or received in an electronic form

PII - Personally Identifiable Information, which makes it possible, either directly or indirectly, the identification a person to whom the information relates

PHR - Personal Health Record is a collection of an individual's health-related information. PHR data include electronic patient health information and personal identification information

DDoS - Distributed Denial of Service technique that uses numerous hosts to perform the attack

AES - Advanced Encryption Standard

LEA - Lightweight Encryption Algorithm

FDA - The United States Food and Drug Administration is a government agency that regulates food and drug products in the United States

HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law to protect sensitive patient health information from being disclosed without the patient's consent or knowledge

GDPR - The General Data Protection Regulation is a regulation in EU law that governs data protection and privacy in the European Union and the European Economic Area

Table of Contents

1 Introduction 1

1.1 Research Problem Defined 4

1.2 Towards a Data Security and Privacy Risk Management Framework 5

1.3 Research Context 9

1.4 Research Objectives and Questions 10

1.5 Research Approach 11

1.6 Research Contribution 12

1.7 Document Structure 14

2 Literature Review 16

2.1 Introduction 16

2.2 Approach Taken 16

2.2.1 Research Questions Defined 17

2.2.2 Data Sources 18

2.2.3 Search Strings 18

2.2.4 Initial Search 19

2.2.5 First Screening 19

2.2.6 Second Screening 20

2.3 Overview of WBAN Applications 20

2.4 Wireless Body Area Networks in Healthcare Applications 23

2.5 Challenges for Wireless Body Area Network Applications 24

2.6 Security and Privacy Requirements and Attacks for WBAN Applications 26

2.6.1 WBAN Application Attack Types 27

2.6.2 Security and Privacy Requirements for WBAN Applications........................... 29

2.7 Existing Approaches for Addressing Security and Privacy Requirements and Attacks…. 36

2.8 Regulations and Standards.. 41

2.8.1 Regulations 41

2.8.2 Standards... 45

2.8.3 Summary.. 51

2.9 Challenges For Adopting a Security and Privacy Framework 53

2.10 Security and Privacy Risk Management Framework Properties 55

2.11 Research Questions Revisited 59

2.12 Summary.. 62

3 Challenges for Assuring Security and Privacy in Practice 66

3.1 Introduction 66

3.2 Data Collection.. 66

3.2.1 Qualitative Interviews defined... 67

3.2.2 Interview Structure and Question Types.. 67

3.2.3 Organisation Profile... 69

3.2.4 Creating Interview Guide.. 70

3.3 Data Analysis... 73

3.4 Findings 76

3.4.1 Methodological Challenges 76

3.4.2 Organisational Challenges 77

3.4.3 Technical Challenges 77

3.5 Conclusion 79

4 Research Methodology 81

4.1 Introduction 81

4.2 Research Paradigms 81

4.2.1 Positivism 82

4.2.2 Realism 82

4.2.3 Interpretivism 83

4.2.4 Pragmatism 83

4.3 Research Approach 84

4.4 Research Choices 85

4.5 Research Strategies 87

4.5.1 Ethnography 87

4.5.2 Case Study 88

4.5.3 Grounded Theory 88

4.5.4 Action Research 88

4.5.5 Design Research 90

4.5.6 Action Design Research 92

4.6 Application of Action Design Research 95

4.7 Data Collection Methods 98

4.8 Summary of Methods, Strategies and Choices 99

4.9 Action Design Research Applied 101

4.10 Research Quality 104

4.10.1 Reliability 104

4.10.2 Validity 105

4.11 Summary 107

5 Development of the WBANSecRM Framework 110

5.1 Development of the Data Security and Privacy Guidelines 111

5.1.1 Control Collection 112

5.1.2 Control Selection 113

5.1.3 Development of Security and Privacy Control Implementation Details 113

5.2 Structure of the Alpha Version of the WBANSecRM Framework 115

5.3 Implementation Process of the Alpha Version 117

5.4 Implementation of the Alpha Version Within an Industrial Setting 118

5.4.1 Scope and Application Use-Case 119

5.4.2 Develop Data Flow Diagram 119

5.4.3 Apply Threat Modelling 119

5.4.4 Implementation of the Controls 122

5.4.5 Evaluate the Effectiveness of the Controls 123

5.5 Development of the Beta Version 125

5.6 Structure of the WBANSecRM Framework Beta Version 127

5.6.1 Security and Privacy Risk Assessment 129

5.6.2 Security and Privacy Risk Controls 130

5.6.3 Evaluation of Overall Residual Security and Privacy Risk Acceptability........ 134

5.7 Summary... 137

6 Data Security and Privacy Risk management Framework (Beta Version) – Expert Review… 141

6.1 Approach to the Expert Review of the Data Security and Privacy Risk management Framework (Beta Version) 141

6.2 Develop Questionnaire 142

6.3 Recruiting Experts and Participant Profiles.. 146

6.4 Methodology for Analysing Expert Review Comments 147

6.5 WBANSecRM framework – Expert Review Comments 150

6.5.1 Security and Privacy Risk Analysis... 151

6.5.2 Evaluate Security and Privacy Risks 157

6.5.3 Security and Privacy Risk Controls 159

6.5.4 Evaluation of Security and Privacy Risk Controls 164

6.5.5 Usability and Efficacy.. 167

6.5.6 General... 172

6.6 Changes to the WBANSecRM Framework As a Result of Expert Review 175

6.7 List of Future Work for WBANSecRM Framework As a Result of Expert Review……………. 177

6.8 Summary... 178

7 Discussion 181

7.1 Introduction 181

7.2 Research Objectives and Question Revisited 181

7.2.1 Objective 1 181

7.2.2 Objective 2 184

7.2.3 Research Question Revisited 188

7.3 Implications of Findings 191

7.3.1 Theoretical Implications 191

7.3.2 Practical Implications 192

7.4 Threats to Validity 194

7.4.1 Reliability 194

7.4.2 Validity 195

7.5 Summary 197

8 Conclusion 200

8.1 Introduction 200

8.2 Summary 200

8.3 Research Contribution 203

8.3.1 Contribution of Knowledge to WBAN Application Security and Privacy Research Community 203

8.3.2 Contribution of Knowledge to WBAN Application Development Community……. 204

8.3.3 Contribution of Knowledge to the Security and Privacy Risk Management Community 205

8.3.4 Lessons Learned as a Result of this Research 206

8.4 Future Research 207

8.5 Conclusion 208

9 References 212

Appendix A Mapping of Occurrence of Security and Privacy Requirements for WBAN Applications 236

Appendix B Structure of WBANSecRM Beta Version 268

Appendix C Implementation Guideline for Security and Privacy Controls 320

Appendix D Case Study of a Fitness Tracking Application 349

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application 369

Appendix F Expert Review Questionnaire 376

Appendix G Interview Questionnaire 384

Table of Figures

FIGURE 1-1 A GENERAL ARCHITECTURE OF WBAN APPLICATION (LI, LOU AND REN, 2010) 1

FIGURE 1-2 RELATIONSHIP BETWEEN RESEARCH ELEMENTS AND THE RESEARCH QUESTIONS AND OBJECTIVES 11

FIGURE 2-1: STEPS TAKEN IN CONDUCTING THE LITERATURE REVIEW 16

FIGURE 2-2: PAPER SELECTION PROCESS DURING THE LITERATURE REVIEW 20

FIGURE 2-3: CATEGORIES OF WBAN APPLICATIONS BY IEEE 802.15.6 STANDARD (KWAK, ULLAH AND ULLAH, 2010) 21

FIGURE 2-4: ATTACK LANDSCAPE BASED ON OCCURRENCES FOR WBAN APPLICATIONS THROUGHOUT 2008-2021 29

FIGURE 2-5: RELATIONSHIP BETWEEN INFORMATION SECURITY AND PRIVACY (NISTIR 8062) 30

FIGURE 2-6: SECURITY AND PRIVACY REQUIREMENTS LANDSCAPE BASED ON OCCURRENCES FOR WBAN APPLICATIONS THROUGHOUT 2008-2021 35

FIGURE 3-1: INTERVIEW QUESTIONNAIRE DEVELOPMENT METHOD 71

FIGURE 3-2: METHODOLOGY FOR ANALYSING INTERVIEW RESPONSE 73

FIGURE 4-1: RESEARCH CHOICES 86

FIGURE 4-2: MODEL OF ACTION RESEARCH (GIVEN, 2008) 89

FIGURE 4-3: STAGES AND PRINCIPLES OF ACTION DESIGN RESEARCH METHOD (MAUNG K. SEIN *ET AL.*, 2011) 93

FIGURE 4-4: BIE DIAGRAM FOR DEVELOPING A DATA SECURITY FRAMEWORK 96

FIGURE 4-5: ACTION DESIGN RESEARCH APPLIED TO THIS RESEARCH 101

FIGURE 5-1: DEVELOPMENT APPROACH OF THE WBANSECRM FRAMEWORK 110

FIGURE 5-2: DATA SECURITY AND PRIVACY CONTROL IMPLEMENTATION DETAILS DEVELOPMENT PROCESS 112

FIGURE 5-3: IMPLEMENTATION PROCESS OF THE DATA SECURITY AND PRIVACY FRAMEWORK (ALPHA VERSION) 117

FIGURE 5-4: FITNESSX DFD DIAGRAM 121

FIGURE 5-5: STRUCTURE OF THE WBANSECRM FRAMEWORK (BETA VERSION) 128

FIGURE 5-6: STEPS TO CONDUCT A SECURITY AND PRIVACY RISK ASSESSMENT 129

FIGURE 5-7: SELECTION AND IMPLEMENTATION PROCESS OF SECURITY AND PRIVACY RISK CONTROL 131

FIGURE 5-8: STEPS FOR EVALUATING THE OVERALL RESIDUAL SECURITY AND PRIVACY RISK ACCEPTABILITY 135

FIGURE 6-1: WBANSECRM FRAMEWORK EXPERT REVIEW APPROACH 142

FIGURE 6-2: EXPERT REVIEW QUESTIONNAIRE DEVELOPMENT METHOD 143

FIGURE 6-3: METHODOLOGY FOR ANALYSING EXPERT REVIEW COMMENTS 148

FIGURE 7-1: INDUSTRIAL IMPLEMENTATION 184

FIGURE 7-2: VALIDATION BY EXPERT REVIEW 187

FIGURE APPENDIX D-1: LIST OF ASSETS FOR FITNESSX SYSTEM 352

FIGURE APPENDIX D-2: THE SYSTEM ARCHITECTURE OF THE FITNESSX APPLICATION 357

FIGURE APPENDIX D-3: DFD DIAGRAM IN MICROSOFT THREAT MODELLING TOOL 359

FIGURE APPENDIX D-4: FITNESSX APPLICATION DISRUTPION ATTACK TREE MODEL 361

Table of Tables

TABLE 1-1: CHALLENGES FACE BY DEVELOPERS FOR ASSURING SECURITY AND PRIVACY 4

TABLE 1-2 RESEARCH OBJECTIVES 10

TABLE 1-3 RESEARCH SUB-QUESTIONS 10

TABLE 2-1: INCLUSION AND EXCLUSION CRITERIA 19

TABLE 2-2: COMPARISON BETWEEN WSN AND WBAN APPLICATIONS (SAMANEH MOVASSAGHI *ET AL.*, 2014) 22

TABLE 2-3: TYPES OF ATTACKS FOR WBAN APPLICATIONS IN CURRENT LITERATURE 27

TABLE 2-4: LIST OF SECURITY AND PRIVACY REQUIREMENTS WITH A DESCRIPTION FOR WBAN APPLICATIONS 30

TABLE 2-5: MAPPING OF OCCURRENCE OF SECURITY AND PRIVACY REQUIREMENTS FOR WBAN APPLICATIONS IN CURRENT LITERATURE 33

TABLE 2-6: MAPPING OF FRAMEWORK OR SOLUTION APPROACH WITH SECURITY AND PRIVACY REQUIREMENTS FOR WBAN APPLICATIONS 36

TABLE 2-7: CHALLENGES FOR ADOPTING SECURITY AND PRIVACY FRAMEWORK (LITERATURE REVIEW) 54

TABLE 2-8: COMPARISON OF THE RISK MANAGEMENT FRAMEWORK PHASES 57

TABLE 3-1 DIFFERENCES BETWEEN INDUCTIVE AND DEDUCTIVE APPROACH 84

TABLE 3-2: DIFFERENT ROLE OF ACTORS IN ACTION RESEARCH DURING THREE PHASES OF RESEARCH (JÄRVINEN, 2012) 89

TABLE 3-3: DIFFERENT ROLE OF ACTORS IN DESIGN RESEARCH DURING THREE PHASES OF RESEARCH (JÄRVINEN, 2012) 91

TABLE 3-4: OVERVIEW OF RESEARCH PROCESS 100

TABLE 5-1: TOPICS REDEFINED TO CATEGORIES FOR DEVELOPING THE QUESTIONNAIRE 144

TABLE 5-2: ILLUSTRATION OF SECURITY AND PRIVACY RISK CONTROL CATEGORY SUB-CATEGORY AND UNIT OF DATA 150

TABLE 5-3: NO OF COMMENTS PER CATEGORY 151

TABLE 5-4: LIST OF EXPERT REVIEW COMMENTS FOR SECURITY AND PRIVACY RISK ANALYSIS 151

TABLE 5-5: LIST OF EXPERT REVIEW COMMENTS FOR EVALUATE SECURITY AND PRIVACY RISK 157

TABLE 5-6: LIST OF EXPERT REVIEW COMMENTS FOR SECURITY AND PRIVACY RISK CONTROL 159

TABLE 5-7: LIST OF EXPERT REVIEW COMMENTS FOR EVALUATION OF SECURITY AND PRIVACY RISK CONTROLS 164

TABLE 5-8: RESPONSES TO THE WBANSECRM FRAMEWORK USABILITY AND EFFICACY 168

TABLE 5-9: LIST OF EXPERT REVIEW COMMENTS FOR USABILITY AND EFFICACY OF WBANSECRM FRAMEWORK 169

TABLE 5-10: LIST OF EXPERT REVIEW COMMENTS FOR GENERAL CATEGORY 173

TABLE APPENDIX E-1: LIST OF ASSETS, THREATS, VULNERABILITY, AND RESPECTIVE CONTROLS FOR WBAN APPLICATION 369

Related Peer Reviewed Publications

Conference Papers

Duc, A.N., Jabangwe, R., **Paul, P.** and Abrahamsson, P., 2017, May. Security challenges in IoT development: A software engineering perspective. In *Proceedings of the XP2017 Scientific Workshops* (p. 11). ACM.

McCaffery, F., Özcan-Top, Ö., Treacy, C., **Paul, P.**, Loane, J., Crilly, J. and Mc Mahon, A., 2018, September. A Process Framework Combining Safety and Security in Practice. In *European Conference on Software Process Improvement* (pp. 173-180). Springer, Cham.

Paul, P.C., Loane, J., Regan, G. and McCaffery, F., 2019, September. Analysis of Attacks and Security Requirements for Wireless Body Area Networks-A Systematic Literature Review. In *European Conference on Software Process Improvement* (pp. 439-452). Springer, Cham.

Paul, P.C., Loane, J., McCaffery, F. and Regan, G., 2019, October. A Serverless Architecture for Wireless Body Area Network Applications. In *International Symposium on Model-Based Safety and Assessment* (pp. 239-254). Springer, Cham.

Regan, G., Mc Caffery, F., **Paul, P.C.**, Reich, J., Sorokos, I., Armangeud, E., Zeller, M. and Longo, S., 2020, September. Achieving Data Privacy with a Dependability Mechanism for Cyber Physical Systems. In *European Conference on Software Process Improvement* (pp. 511-524). Springer, Cham.

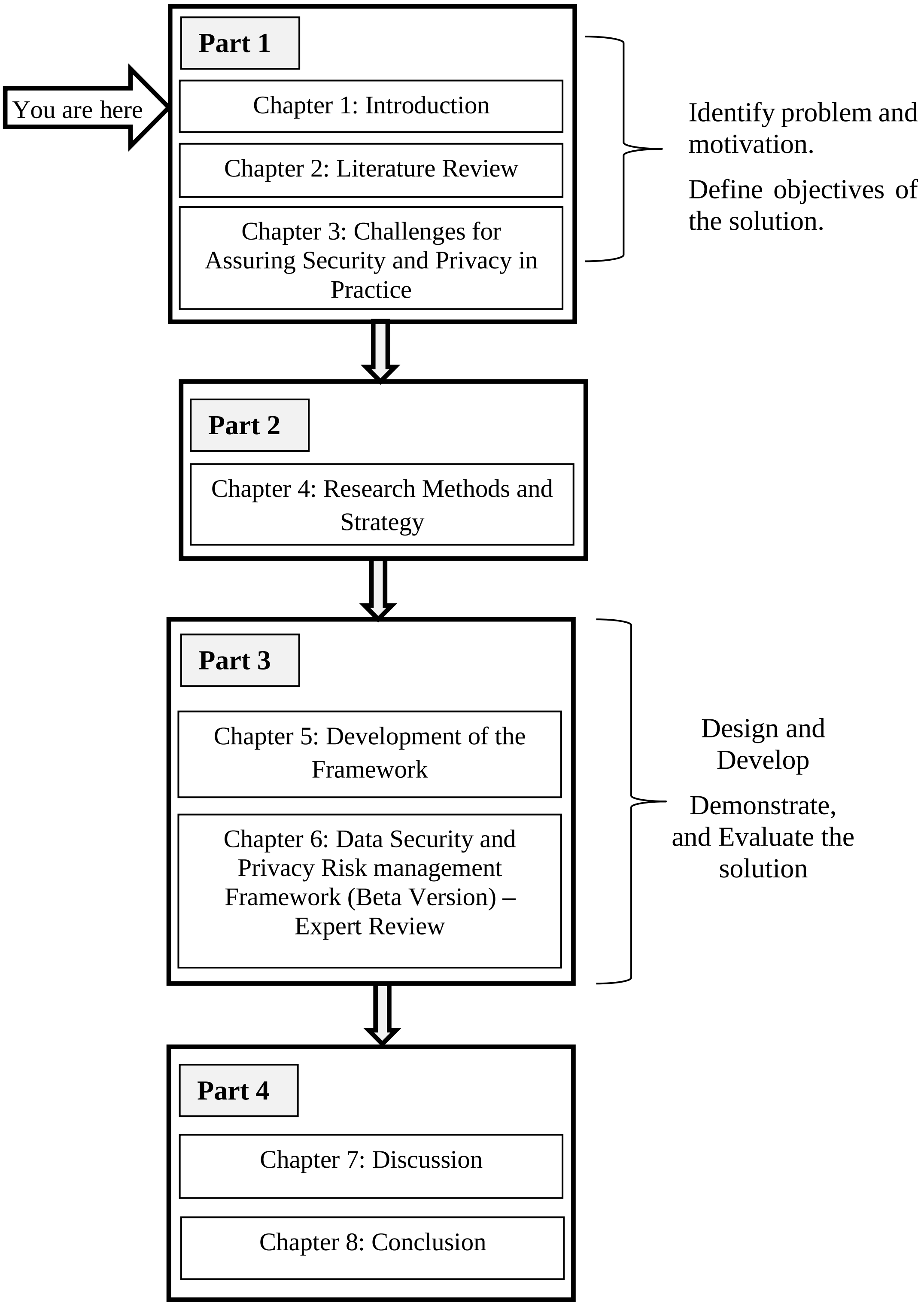
Paul, P.C., Loane, J., McCaffery, F. and Regan, G., 2021, March. A Data Security And Privacy Risk Management Framework For WBAN Based Healthcare Applications. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (pp. 704-710). IEEE.

Journal Papers

Regan, G., McCaffery, F., **Paul, P.C.**, Reich, J., Armengaud, E., Kaypmaz, C., Zeller, M., Guo, J.Z., Longo, S., O'Carroll, E. and Sorokos, I., 2020. Quality improvement mechanism for cyber physical systems—An evaluation. *Journal of Software: Evolution and Process, 32*(11), p.e2295.

Paul, P.C., Loane, J., McCaffery, F. and Regan, G., 2021. Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications. *Applied System Innovation*, 4(4), p.76.

Map of Thesis


You are here
Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

1 Introduction

A Wireless Body Area Network (WBAN) application comprises intelligent, low-power sensor nodes that monitor body functions and physiological states. These sensor nodes can collect and process data, store it locally and transmit it to an actuator or a local server. Generally, a WBAN application can consist of two types of body area networks: in-body and on-body area networks. An in-body network allows communication between invasive or implanted sensor devices and a base station. Similarly, the on-body network allows communication between the wearable sensor device and a base station (Ullah *et al.*, 2012).

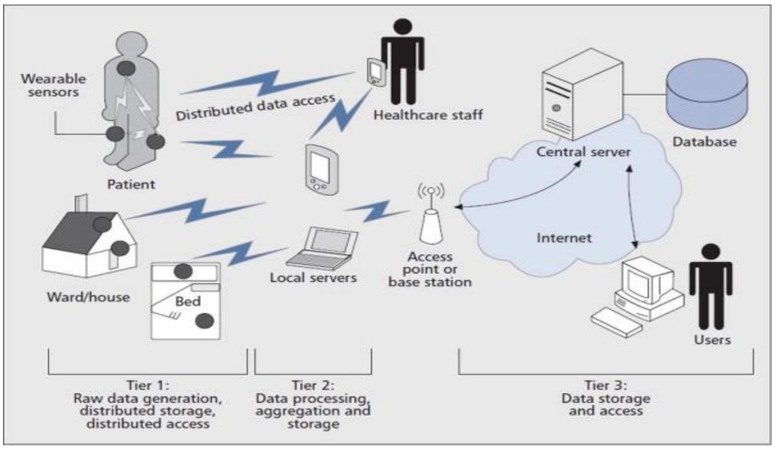

Wearable sensors
Distributed data access
Healthcare staff
Central server
Database
Patient
Internet
Access point or base station
Ward/house
Local servers
Bed
Users
Tier 1: Raw data generation, distributed storage, distributed access
Tier 2: Data processing, aggregation and storage
Tier 3: Data storage and access

Figure 1-1 A general architecture of WBAN application (Li, Lou and Ren, 2010)

Usually, WBAN applications consist of three types of device; a sensor node, a central control unit (CCU) and a mobile node (Salehi *et al.*, 2016). A general architecture for WBAN applications is illustrated in Figure 1-1. In Figure 1-1, tier 1 represents the data generation unit which consists of one or more sensor nodes. A sensor node uses different biosensors to collect vital physiological signs in the human body. These sensor nodes contain a processor, transceiver, power unit and internal storage unit. Tier 2 in Figure 1-1 consists of a personal digital assistant (PDA) or a computer which is used as a mobile node and works as a gateway to transfer information to its destination. This mobile node will receive all data from the sensor nodes or CCU and transmit it to a central server through the internet using Worldwide Interoperability for Microwave Access (WiMAX), General Packet Radio Service (GPRS) and

Global System for Mobile Communications (GSM). Tier 3 consists of a database and server used to store the data and provide access to the data using an application.

The IEEE 802.15.6 - *IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks* (IEEE 802.15.6, 2012) categorises WBAN applications into two categories; medical and non-medical applications. Medical applications consist of healthcare solutions for aging and diseased populations. Early diagnosis, prevention, and monitoring of illnesses, geriatric care at home, post-surgery rehabilitation, biofeedback programs that manage emotional states, and assisted living applications that enhance the quality of life for persons with impairments are examples of medical applications (Negra, Jemili and Belghith, 2016). On the other hand, applications like motion and gesture detection for interactive gaming and fitness tracking apps, cognitive and emotional identification for driving assistance or social interactions, and medical support in catastrophe situations are examples of non-medical uses (Rismanian, Hosseinzadeh and Jabbehdari, 2017).

The use of WBANs for medical applications is aimed at providing continuous monitoring of an individual's physiological attributes, such as blood pressure, heartbeat and body temperature. Wang *et al.* (2016) classified WBAN based healthcare applications into two subcategories; On-Body and In-Body WBAN. On-Body WBAN healthcare applications use wearable sensor nodes to observe patient health in real-time. In-Body based applications use the implanted sensor in the human body, either underneath the skin or in the blood stream to observe patient health in real-time. WBAN systems can monitor the postural balance and stability of athletes in real time and provide valuable feedback to the coaches and trainers which can help minimise injury to athletes and maximise their playing potential (Chakraborty, 2018). Additionally, this kind of system provides data logging capability. This data logging capability assists the analyst and the coach in monitoring past performances of athletes and thus helps in determining the level of injury that an athlete is currently suffering, and thereby helps determine if injuries are career threatening.

Data security and privacy of patient’s health records (PHR) are two essential components for WBAN applications. PHR data include electronic patient health information and personal identification information. Data security means assuring that data is protected from unauthorised users while the data is being collected, processed, stored and transmitted. Data privacy confers a right for individuals to control the collection and use of personal health information. The main design requirements for any WBAN application is that the body sensor node needs to be extremely small and thin, capable of wireless communication, and use minimal power for data collection and processing (Antonescu and Basagni, 2013). User requirements such as privacy, safety, ease of use, security and compatibility are also of great importance (Salayma et al., 2017).

WBAN applications operate in an environment where many people have open internet access which leaves them vulnerable and open to many types of attacks and threats. Open connectivity creates a large attack surface. Attacks can affect the performance and availability of the service, sometimes leading to life threating situations (Kotz, 2011). Furthermore, security and privacy are regulatory requirements that also need to be considered during development of healthcare applications. While many techniques have been proposed for addressing security and privacy, they are not particularly suited to WBAN due to the resource constraints in terms of power, memory and computational capability (Samaneh Movassaghi *et al.*, 2014). As complex security mechanisms require more computation and power resources, it is necessary to have a solution that minimises both (Chin *et al.*, 2012).

Therefore, considering the importance of assuring data security and privacy the focus of this study is to find a way to assist developers to identify and implement the safeguards for assuring security and privacy effectively.

1.1 Research Problem Defined

This study includes an extensive literature review which was conducted in order to identify the challenges related to WBAN application development. The literature review indicates various challenges for WBAN applications which are; energy efficiency, antenna design, quality of service and, security and privacy. The literature review indicates that a security and privacy breach in a WBAN based healthcare application not only costs money; in some cases, it can create a life-threatening event. So, security and privacy safeguards need to be considered during the development of this type of healthcare application. Furthermore, medical devices need to be compliant with various legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). Assuring security and privacy is a key requirement of compliance. To corroborate these challenges, an interview was conducted by the author of this study with a WBAN development organisation. The organisation indicated that while each of the above challenges existed for them, concerns around implementing security and privacy were to the forefront. They stated that they have a high demand for data security and privacy because their product collects and analyses sensitive PHR data. This feedback determined the focus of this study which is to find a way of assisting organisations to develop WBANs that meet security and privacy requirements. The list of challenges faced by developers for assuring security and privacy identified from both the literature review and interview are presented in Table 1-1:

Table 1-1: Challenges face by developers for assuring security and privacy

Challenges	Sources
Lack of trained staff, responsibilities, budget, and management support	**Literature & Interview** (Townsend, 2017), (Holden, 2014), MacMahon et al., (2018), (Q. Chen et al., 2016) (Shah and Khan, 2020), (Eom and Lee, 2017) (Benz and Chatterjee, 2020), (Chen and Benusa, 2017) (Mariani and Mohammed, 2015), Ključnikov et al., (2019)
The existing standards are too complex and complicated to implement	**Literature & Interview** MacMahon et al., (2018), (Eom and Lee, 2017) (Aljohani and Blustein, 2018), (Skierka, 2018) (Thapa and Camtepe, 2021)

Challenges	Sources
Limited knowledge about market-specific regulatory requirements, security standards, and policies	**Literature & Interview** (Chen and Benusa, 2017), (Skierka, 2018) (Supriya and Padaki, 2016), Stevovic et al., (2013) Abraham et al., (2019)
Lack of comprehensive understanding of the architecture for WBAN security and privacy	**Interview**
Understanding the data flow around the system and what assets need to be protected	**Interview**
Standards outline each security control at a very high-level with limited amount of implementation details	**Literature & Interview** MacMahon et al., (2018), (Mariani and Mohammed, 2015)
Identification of appropriate security controls with respective implementation details to assure confidentiality, integrity, availability and privacy of data	**Literature & Interview** Aceto et al., (2018)
Due to a vast number of controls, the challenge is prioritizing these controls in addition to planning releases without compromising security and privacy	**Interview**
Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage	**Literature & Interview** (Thapa and Camtepe, 2021) (Supriya and Padaki, 2016) Iyengar et al., (2018) Paquette et al., (2011)

1.2 Towards a Data Security and Privacy Risk Management Framework

A Risk Management Framework (RMF) is a process that provides a comprehensive approach to managing security, privacy, and cyber supply chain risks during the system development life cycle (NIST RMF, 2023). A RMF promotes security and privacy awareness and helps organisations proactively address potential threats. By adopting a RMF, stakeholders can communicate transparently and understand their roles and responsibilities in risk management. A RMF plays a crucial role in facilitating compliance with pertinent laws, regulations, and industry standards by carefully identifying the relevant requirements and implementing suitable controls to mitigate any potential security risks (Kim and Solomon, 2021, pp.248). A RMF also enables the establishment of robust governance structures that guarantee accountability and oversight in managing security risks, ensuring that an organization's security posture remains strong and resilient.

A RMF is also an essential tool for organisations to evaluate and manage risks effectively. It enables a thorough understanding of the threat landscape, including the likelihood and potential impact of various risks (ISO 27005, 2015). A RMF also provides visibility into security risks and their potential impact on business objectives, which helps in making informed decisions. It emphasises the significance of the framework in enabling executives to oversee the organisation's security posture effectively, ensuring alignment with strategic goals and objectives (Touhill and Touhill, 2014, pp.8). By leveraging a framework, senior leadership can make informed decisions about resource allocation, risk mitigation strategies, and investments in security measures. By prioritising and addressing the most critical risks first, the RMF helps organisations safeguard their assets and resources, minimize vulnerabilities, and ensure business continuity. The RMF also help organisations to assure that their resources are utilised efficiently and effectively in addressing the most critical risks first (Hubbard, 2020, pp.11-12).

By having a well-defined and structured risk management framework in place, organisations can respond quickly and effectively to security and privacy incidents. This framework facilitates a coordinated and systematic approach, ensuring that all necessary stakeholders are involved, and that the response is well-coordinated (NIST SP 800-61, 2024). A RMF plays a crucial role in facilitating regular reviews and updates of organisations' risk management processes in response to evolving threats and changes in the business environment. This process of continuous improvement is crucial for ensuring that security and privacy measures remain effective over time. According to research conducted by Whitman et al. (2017, pp.24), adaptability and continuous improvement are of utmost importance in security and privacy risk management practices.

Implementing security frameworks like the NIST Cybersecurity Framework or ISO/IEC 27001 can help organisations manage security risks in a structured way. These frameworks offer guidelines for identifying and managing security risks throughout the organisation needs (NIST CSF, 2021)(ISO/IEC 27002, 2017). An alternative to traditional risk management frameworks for security and privacy is the zero-trust security model. The zero-trust security model assumes threats from both inside and outside the network and requires verification for anyone accessing resources. It provides a robust security and privacy solution based on continuous authentication, strict access controls, and least privilege access (Gilman and Barth, 2017, pp. 1-6). Another alternative approach is the Privacy by Design (PbD) framework. The PbD is a methodology that involves integrating privacy safeguards into the design and architecture of systems, processes, and technologies from the very beginning, rather than as an afterthought or add-on solution (Cavoukian, Taylor and Abrams, 2010). This framework prioritizes proactive measures to ensure privacy, instead of reactive responses to privacy breaches. A resilience-focused approach is a strategic approach that aims to make an organization more adaptable to the uncertain and rapidly changing business environment. It is an alternative to traditional risk management, which focuses solely on identifying and mitigating risks. In contrast, resilience is about building systems and processes that can quickly adapt and recover from unexpected events or disruptions (Bejtlich, 2013). The Zero-trust security model was not considered as the implementation of the Zero-trust security model in healthcare applications can be a complex process. It often requires significant changes to network architectures, policies, and workflows to comply with regulatory requirements. Additionally, the implementation of PbD was not considered due to the technical expertise and resources required to integrate privacy features into existing systems or to design new systems with privacy in mind. This process can be complex and may require a significant investment of time, money, and manpower.

Upon analysing the options, I choose to develop a risk management framework. This framework will facilitate a systematic approach to identifying, assessing, and managing any potential risks that may emerge over the course of the application's life cycle. The framework will be designed to provide a comprehensive approach to risk management, incorporating a range of tools and techniques to identify and evaluate potential risks effectively. By systematically identifying and analysing risks, organisations will be able to prioritise and allocate resources effectively to manage them. This leads to better decision-making, as organisations can make informed choices based on accurate risk assessments. Additionally, this framework will help organisations to build resilience by anticipating potential risks and developing mitigation strategies.

The literature review resulted in a total of four risk management frameworks: ISO/IEC 80001-1:2010, AAMI TIR57, ISO 14971 and NIST 800-30. An initial analysis found that only two of these four frameworks were 'healthcare specific' security and privacy risk management frameworks, that is ISO/IEC 80001-1:2010 and AAMI TIR57. Further analysis of the ISO/IEC 80001-1:2010 and AAMI TIR57 found that neither of these frameworks were suitable for developing WBAN applications. IEC 80001-1:2010 was primarily developed for applications which operate within a healthcare delivery organization's IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media. AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices. AAMI TIR57 was developed with guidelines provided by ISO 14971 and NIST SP 800-30. This framework does not provide any guidance for managing security and privacy risks for resource-constrained sensor devices. A WBAN application consists of resource constrained sensor devices which have limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications. Neither framework provides any guidance for managing security and privacy risks for resource constrained sensor devices.

Considering the challenges that organisations and developers face for assuring security and privacy of PHR data followed by the outcome of the literature review, a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Application (WBANSecRM framework) has been developed as part of this study. The aims of the WBANSecRM framework are that:

- It should provide a clear pathway for developers to assure data security and privacy, and assist them to fulfil the medical device security and privacy related regulations

- It should assist medical device development organisations who have limited resources and expertise in this area to assure security and privacy

The WBANSecRM framework consists of three key elements – a risk assessment process to identify the threats and vulnerabilities, a list of WBAN security and privacy controls with implementation details, and a process to evaluate the effectiveness and efficacy of the controls. This framework provides a list of assets, threats and vulnerabilities that apply to WBAN applications. This list of assets, threats and vulnerabilities will assist WBAN development organisations in conducting the risk assessment process. The implementation details for each security and privacy control were extracted from various standards and best practice guidelines. As standards and guidelines provide insufficient implementation details, this framework uses additional standards, external sources, research papers and blogs to further define implementation details for each control.

The focus of this study is on the development and evaluation of the WBANSecRM framework, which will provide the answer to the following overall research question:

"How can the development of a data security and privacy risk management framework for wireless body area network (WBAN) based healthcare applications assist developers and organisations in improving the security and privacy of data, and put them on the road to regulatory compliance?"

1.3 Research Context

The focus of this study is on organisations that develop WBAN based healthcare applications. The sensor-based healthcare application market size was valued at USD 5.69 billion in 2020 and expected to reach USD 10.11 billion by 2026, with a compound annual growth rate of 10.07% (Researchandmarkets, 2021). The Body Area Network market is anticipated to increase from USD 9.09 billion in 2018 to USD 21 billion by 2025, at a CAGR of 13%, according to Market Research Future (MRFR) (Marketresearchfuture, 2021). The healthcare industry is faced with the constant challenge of complying with stringent healthcare regulations and assuring security and privacy while also providing quality healthcare to patients. Therefore, this study is motivated by the following aspects:

- The importance of WBAN based healthcare applications and the desire to assist medical device organisations to assure security and privacy and put them on the path to regulatory compliance
- Organisation's lack of security and privacy expertise
- Non-medical applications such as an 'athletic tracking application' do not need to comply with the same stringent requirements as medical applications, however non-medical applications still need to comply with security and privacy requirements as they collect, process and store PHR data

1.4 Research Objectives and Questions

In order to answer the main research question, this study was divided into two distinct but equally important objectives as detailed in Table 1-2:

Table 1-2 Research Objectives

Objective	Research Objectives
1	**RO 1:** To design and develop a Data Security and Privacy Risk Management Framework which will assist developers in assuring security and privacy of WBAN based healthcare applications.
2	**RO 2:** To validate the Data Security and Privacy Risk Management Framework.

To meet these objectives, four research sub-questions have been identified which are detailed in Table 1-3.

Table 1-3 Research Sub-Questions

Objective	Research Sub-Questions
1	***RSQ 1:*** What challenges are faced by developers of wireless body area network applications in assuring the security and privacy of PHR data?
	RSQ 2: What frameworks, methods and techniques are used to assure data security and privacy for wireless body area networks?
	RSQ 3: What should a WBANSecRM framework contain to assist wireless body area network application developers in assuring security and privacy and put them on the path to regulatory compliance?

2	***RSQ 4:*** To what extent can the WBANSecRM framework address the challenges faced by developers in assuring data security and privacy while developing WBAN based healthcare applications?

1.5 Research Approach

The research approach taken to address each objective and research sub-question is presented in Figure 1-2. To answer RSQ 1 a literature review was conducted to investigate the challenges faced by the developers for assuring security and privacy while developing a WBAN based application. Additionally, one organisation developing WBAN applications was interviewed to identify the challenges the organisation faces in assuring security and privacy.

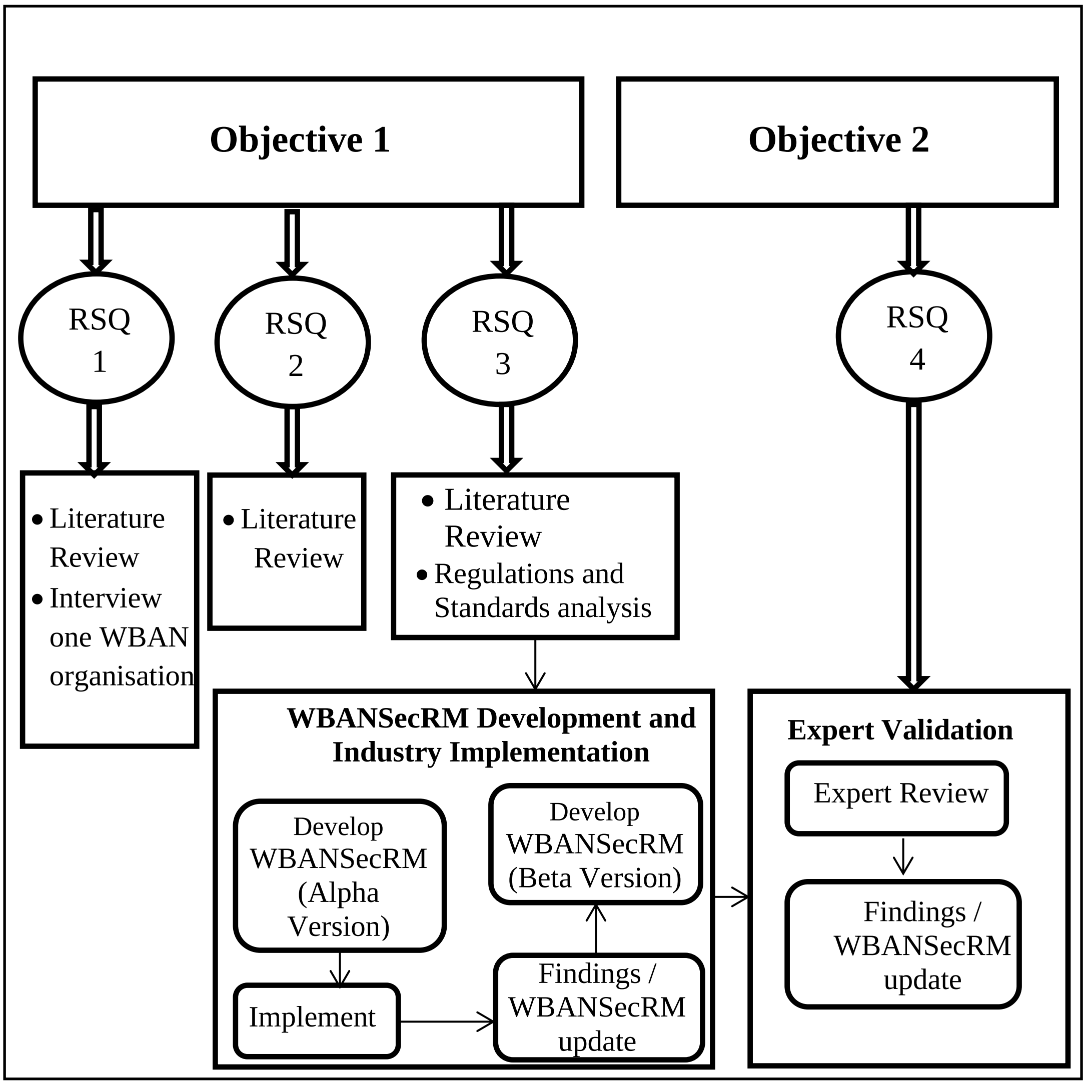

Objective 1
Objective 2
RSQ 1
RSQ 2
RSQ 3
RSQ 4
• Literature Review
• Interview one WBAN organisation
• Literature Review
• Literature Review
• Regulations and Standards analysis
WBANSecRM Development and Industry Implementation
Develop WBANSecRM (Alpha Version)
Implement
Findings / WBANSecRM update
Develop WBANSecRM (Beta Version)
Expert Validation
Expert Review
Findings / WBANSecRM update

Figure 1-2 Relationship between Research Elements and the Research Questions and Objectives

To address RSQ 2, a literature review was conducted to understand available methods, techniques and best practices to assure security and privacy of WBAN applications. To answer RSQ 3, an analysis of the existing regulations and standards within the healthcare application domain was conducted to identify the security and privacy requirements. This analysis helped in determining the countermeasures required for assuring security and privacy. Additionally, a literature review was conducted to identify the properties of a risk management framework, making the framework easy to understand, easy to use, and easily adaptable by organisations. The alpha version of the WBANSecRM framework was developed, consisting of the security and privacy requirements with respective countermeasures required to assure the security and privacy of WBAN based healthcare applications. Upon completion of the development of the alpha version of the WBANSecRM framework, it was then implemented in an industrial setting. The feedback and comments received from the industrial trial were analysed, which resulted in the beta version of the WBANSecRM framework.

To evaluate the usability and efficacy of the WBANSecRM framework and address RSQ 4, the beta version of WBANSecRM framework was validated through expert review by experts from both academia and industry.

1.6 Research Contribution

Assuring data security and privacy is a key challenge in the WBAN based application development process. The literature review and an interview with an organisation that develops a WBAN application highlighted a need for a data security and privacy framework. This research will help developers in assuring data security and privacy, and assist them to develop regulatory compliant WBAN based healthcare applications.

The primary contribution is:

- A data security and privacy risk management framework which will allow WBAN based healthcare developers to:

1. Identify possible threats and vulnerabilities specific to their WBAN application. The WBANSecRM framework includes a list of threats and vulnerabilities which apply to WBAN applications. The list of threats and vulnerabilities will assist developers to understand the threat and vulnerability landscape of WBAN applications
2. The WBANSecRM framework also consists of a step-by-step 'control implementation guide'. This guide will assist developers with minimal security expertise to implement security and privacy controls

Further original contributions of this research include:

- An extensive literature review identified a list of eleven types of attacks and twenty-two types of security and privacy requirements. This list will be useful to developers as it identifies the attack types which developers should consider when developing WBAN applications and also identifies the security and privacy requirements developers need to implement to assure security and privacy and to achieve regulatory compliance
- A list of assets and respective threats and vulnerabilities which apply to WBAN applications. This list of assets and respective threats and vulnerabilities will assist the developer in understanding the threat and vulnerability landscape of WBAN applications
- A list of security and privacy controls with implementation details to mitigate these threats and vulnerabilities. The developer-friendly implementation details will assist the developer in implementing safeguards to mitigate the threats and vulnerabilities. The control's implementation details are extracted from various relevant standards and best practice guidelines. Therefore, the developer does not need to look at multiple

sources to get the implementation details. This will help the organisation reduce development time

This research also contributes to learning through:

- The publication of knowledge gathered during the research (Publications)

1.7 Document Structure

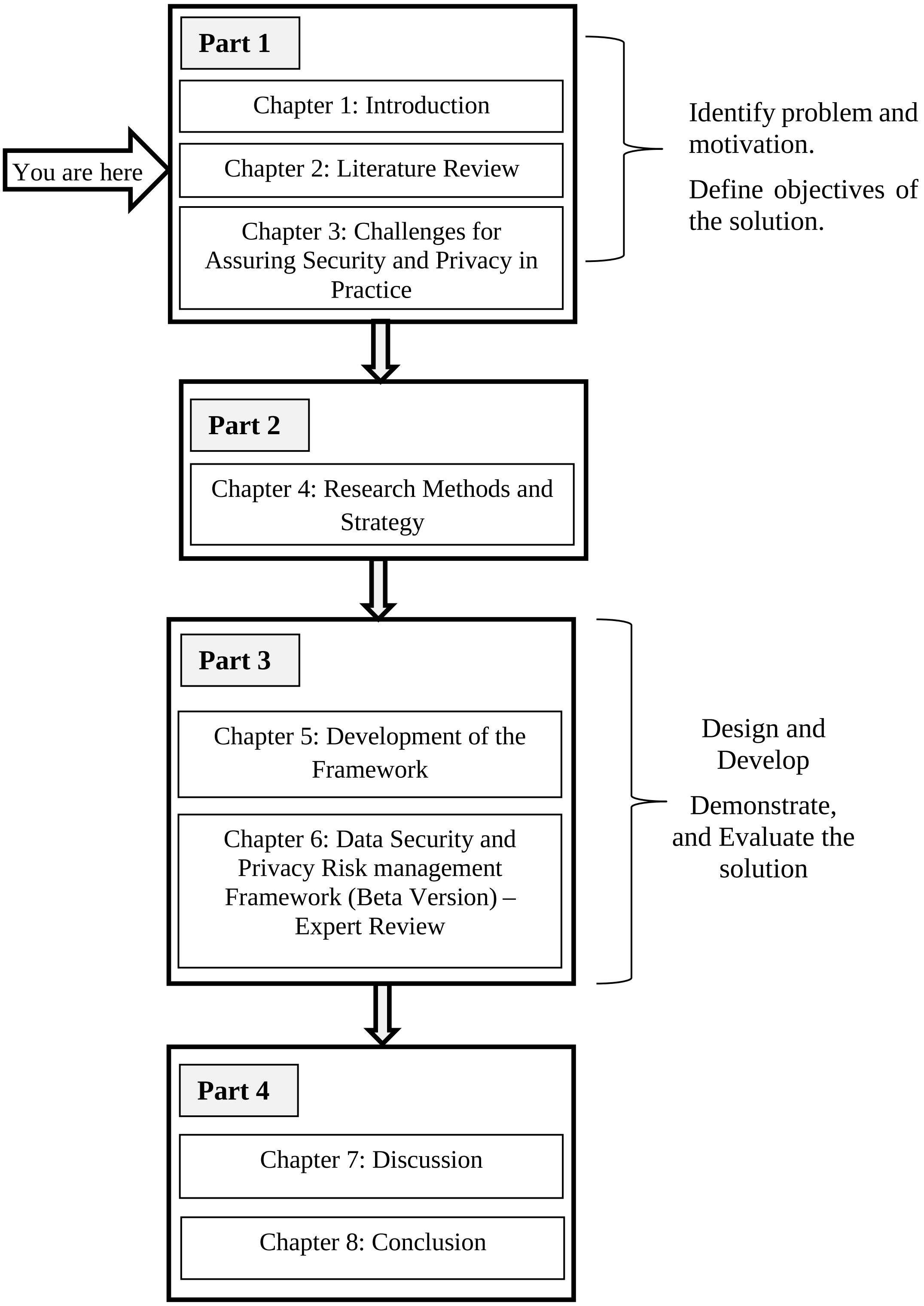
The thesis is organised into four parts. Part 1 contains three Chapters. Chapter 1 is the introduction. The literature review, which is presented in Chapter 2, provides a review of research already undertaken in the area of security and privacy for WBAN applications. Chapter 3 presents the findings from interview with one medical device organistion which conducted in order to identify the challenges for assuring security and privacy.

Part 2 contains one chapter. Chapter 4 presents a review of the principal philosophical approaches to research. Each research method was reviewed in terms of their suitability to conduct and evaluate this research.

Part 3 contains two Chapters. Chapter 5 describes the methodology used to develop the alpha and beta versions of the WBANSecRM framework, presents the structure of the alpha and beta versions, and provides results from the implementation of the alpha version within a WBAN development organisation. Finally, Chapter 6 describes how the beta version of the WBANSecRM framework was evaluated by expert review and presents the results of this evaluation.

Part 4 contains two chapters. Chapter 7 provides a detailed discussion on how the framework assists in assuring security and privacy. Finally, Chapter 8 summarises the contribution of this research, addresses its limitations and also explores directions for future research.

Map of Thesis



Part 1
Chapter 1: Introduction
You are here
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

2 Literature Review

2.1 Introduction

The purpose of this chapter is to provide an in-depth analysis of research already undertaken in the area of WBAN based healthcare applications, with emphasis on security and privacy challenges related to data at rest and data in transit. This chapter begins by outlining the process adopted in conducting this literature review to identify the security and privacy requirements and types of attack for WBANs. Additionally, a review of existing approaches for assuring data security and privacy of WBAN applications is presented. Finally, the chapter concludes with a summary of the security and privacy requirements, attack types, and weaknesses of existing data security and privacy solutions when applied to WBAN applications. This summary shows the need to develop a new framework to assure data security and privacy of a WBAN based healthcare application.

2.2 Approach Taken

This literature review followed the guidelines proposed by Kitchenham et al.(2007). The approach taken to structure the literature review is shown in Figure 2-1.

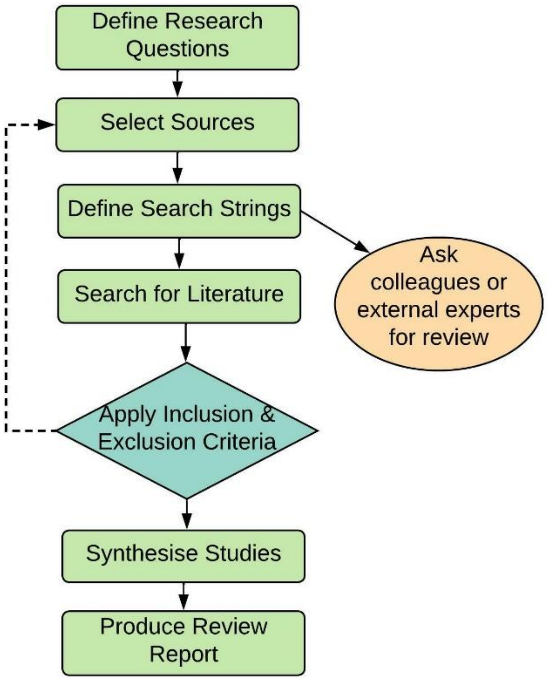

Define Research Questions
Select Sources
Define Search Strings
Ask colleagues or external experts for review
Search for Literature
Apply Inclusion & Exclusion Criteria
Synthesise Studies
Produce Review Report

Figure 2-1: Steps taken in conducting the literature review

2.2.1 Research Questions Defined

This study was motivated by a need to assist WBAN development organisations to assure security and privacy of data at rest and in transit of WBAN healthcare applications. Therefore, the focus of this review was to analyse the challenges in assuring data security and privacy and to provide solutions for one or more of these challenges. This literature review is centred on research sub-questions RSQ 1, RSQ 2, and RSQ 3 which are listed in Section 1.4 of this thesis. These research sub-questions have been further divided into the following questions:

RSQ 1: What challenges are faced by developers of wireless body area network applications to assure the security and privacy of PHR data?

- RSQ1.1: What types of attacks threaten data in WBAN applications?
- RSQ1.2: What are the requirements for assuring data security and privacy in WBAN applications?

RSQ 2: What frameworks, methods and techniques are used to assure data security and privacy for wireless body area networks?

- RSQ2.1: What existing security and privacy frameworks, methods and techniques are used to secure data in WBANs, and what are their limitations?

RSQ 3: What should the WBANSecRM framework contain to assist wireless body area network application developers in assuring security and privacy and put them on the path to regulatory compliance?

- RSQ3.1: What properties should the risk management framework contain to assure security and privacy?
- RSQ3.2: What legislation and standards are available for assuring security and privacy of PHR data in wireless body area networks?

2.2.2 Data Sources

The second step was to choose electronic databases of peer-reviewed papers. The databases should contain literature from key journals and conferences concerning WBAN applications. The following electronic databases were used during the search process:

- IEEE Digital Library (Explore)
- ACM Digital Library
- SpringerLINK
- ScienceDirect (Elsevier)

These databases were selected as the DKIT library provides access to them. If any publications identified in Google Scholar were not available through IEEE, ACM, SpringerLink or ScienceDirect, they were requested through DKIT's inter-library loan service. Additionally, Google Scholar was used as a search engine to find open-access publications. Google Scholar does not allow for the export of large search results, therefore a tool named 'Publish & Perish' was used to export the results.

2.2.3 Search Strings

To identify the relevant primary literature, search strings were designed by using keywords from the research questions. The search strings were used to run a pilot search. The search results were then reviewed with supervisors and colleagues. Through an iterative process the search strings shown below were developed and used during the search process:

- (WBAN OR "wireless body area network" OR "wearable wireless body area network") AND ("security risks" OR "security challenges" OR "security issues" OR "security requirements" OR "privacy risks" OR "privacy challenges" OR "privacy issues" OR "privacy requirements" OR "types of attack")
- (WBAN OR "wireless body area network" OR "wearable wireless body area network") AND ("security framework" OR "privacy framework" OR "data security framework"

OR "security solution" OR "privacy solution" OR "data security solution" OR "security technique" OR "data security technique")

- healthcare AND (security OR privacy) AND (standard OR regulation OR compliance) AND (barrier OR challenges OR difficulties)

2.2.4 Initial Search

The initial search entailed querying each digital library with the search strings and using the inclusion and exclusion criteria presented in Table 2-1. A wide range of papers were returned from the selected databases. Among them, 275 papers were removed due to being duplicates. The duplication occurred as the Google Scholar search results replicated papers found in the other four databases. Removing the duplicate records resulted in a total of 1872 papers. These 1872 papers were recorded in a spreadsheet with a unique record number, article title, abstract, type of publication, publication date, author's name and the number of citations.

Table 2-1: Inclusion and exclusion criteria

Inclusion	Exclusion
- Publication year: 2008-2021 - Language: English - Full text available	- Literature that neither identifies nor addresses data security and privacy challenges, threats, security and privacy requirements or security and privacy frameworks for WBAN applications - Exclude position papers, book reviews, anonymous publications - Exclude duplicate studies

2.2.5 First Screening

The first screening involved an analysis of each paper by reviewing the abstract. If the abstract addressed security and privacy challenges, attacks, security and privacy requirements or security and privacy frameworks for WBAN or sensor-based healthcare applications, it was selected for a second screening. Otherwise, it was discarded. As indicated in Figure 2-2, a total of 742 out of 1872 papers remained after the first screening.

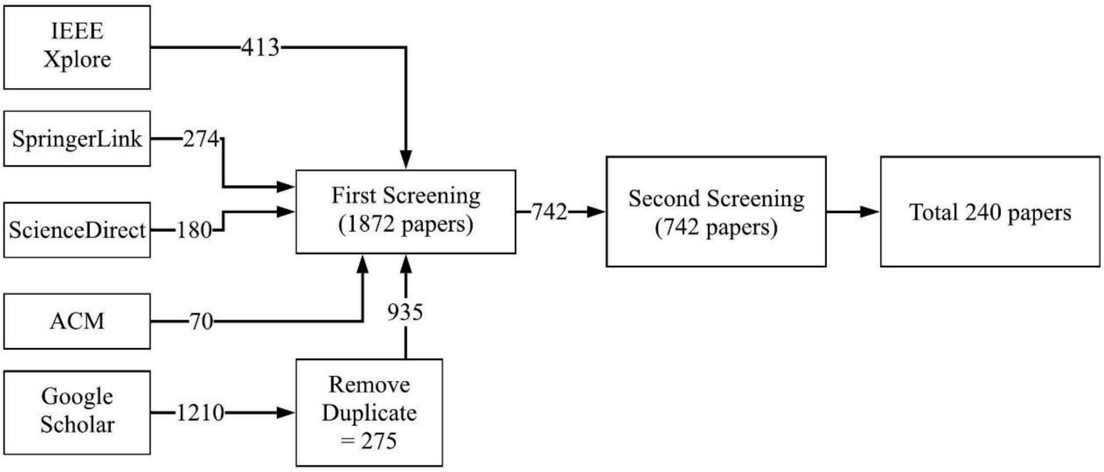


Figure 2-2: Paper selection process during the literature review

2.2.6 Second Screening

In the second screening, individual papers were analysed by reading the full text. In this screening process, research papers were selected for further analysis if the paper presented security and privacy challenges, attacks, security and privacy requirements or frameworks for WBAN or sensor-based healthcare applications. Where multiple terms were used to refer to the same attack or security and privacy requirement, terms are separated with a "/", as indicated in section 2.6.1 and 2.6.2. For example, physical attack and node-compromising attack are used interchangeably in the literature, and in this document they are referred to as physical attack / node-compromising attack. This was achieved by comparing each author's definition of the term. The second screening resulted in a total of 240 relevant papers. Finally, all papers were divided into three categories; 1) papers which addressed security and privacy requirements (207 papers), 2) papers which addressed various attacks (178 papers) and 3) papers which addressed security and privacy framework or solution approaches on WBAN applications (124 papers). If any paper covered multiple categories, it was added into multiple categories.

2.3 Overview of WBAN Applications

WBAN based applications are becoming popular due to the recent advances in sensors, micro-electronics technology and wireless communication. WBAN applications span many domains such as military, ubiquitous healthcare, and sport and entertainment. WBAN applications can also be categorised as medical and non-medical applications as illustrated in Figure 2-3. A WBAN based healthcare application can provide long term health monitoring of a patient's natural physiological states without constraining their normal activities. It also helps to develop a smart, easily accessible and affordable healthcare system. Additionally, a WBAN based healthcare application can also assist with diagnostic procedures, maintenance of chronic conditions, supervised recovery from a surgical procedure and can handle emergency events (Ullah *et al.*, 2012).

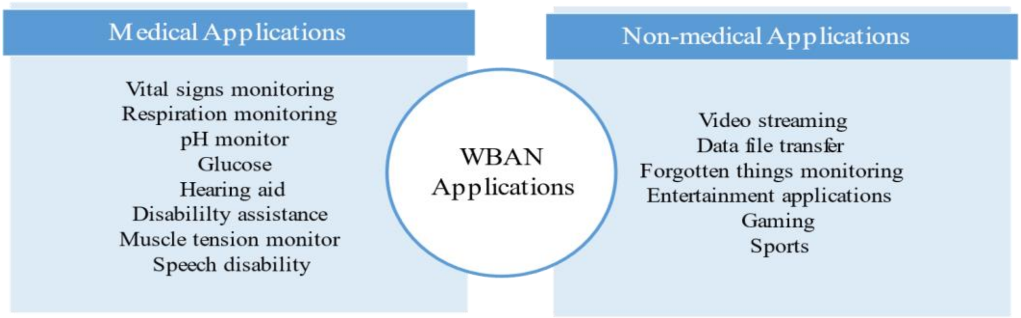


Figure 2-3: Categories of WBAN applications by IEEE 802.15.6 standard (Kwak, Ullah and Ullah, 2010)

WBAN applications include one or multiple medical sensors which can measure a patient's physiological data and transmit this data to a central medical server. This means that a patient can get continuous medical support while residing at home, instead of in-hospital care. In an emergency, this medical sensor can also raise an alarm and send an urgent notification to a nearby medical centre (Arefin, Ali and Haque, 2017). Furthermore, a WBAN application can be very useful for other types of healthcare services which require real-time monitoring such as; glucose level for diabetes control, cancer cell monitoring, and cardiovascular disease monitoring.

Non-medical WBAN based applications include soldier monitoring applications for military and defence, real-time video streaming, gaming and sports applications which are becoming increasingly popular. Advances in gaming have been achieved by integrating different gadgets such as microphones, MP3-players, cameras, displays, and head-mounted routers with advanced computing devices (S Movassaghi *et al.*, 2014). With the help of body sensors, a gamer can control the game using hand and body motion. Additionally, the body sensors can provide feedback to the gaming console which enhances the entertainment experience. WBAN applications can also help athletes to improve their performance and prevent injury. An athlete's fitness can be tracked by using wearable sensors to monitor the physiological activities of the athlete such as blood pressure, heart rate, blood oximetry, navigation, distance and posture (Wang *et al.*, 2016). Similarly, a WBAN based application can play a vital role in the military and defence domain by monitoring soldiers activities, health condition, location, hydration level and surrounding information in real-time. In a battlefield scenario, a health monitoring sensor along with a camera and GPS implemented in a military uniform can provide more accuracy, survivability and connectivity (T and K, 2018).

WBANs are considered a subset of wireless sensor networks (WSNs) due to similarities in network development (Samaneh Movassaghi *et al.*, 2014). However, because of the typical properties of a WBAN application and the unique environment of the human body, current protocols and algorithms of WSN are not always well suited to support a WBAN application (Latré *et al.*, 2011). Table 2-2 illustrates the difference between WSN and WBAN applications.

Table 2-2: Comparison between WSN and WBAN applications (Samaneh Movassaghi *et al.*, 2014)

Comparison criteria	Wireless sensor network	Wireless body area network
Network Dimensions	Few to several thousand nodes over an area from meters to kilometres	Dense distribution limited by body size
Topology	Random, Fixed/Static	One-hop or two-hop star topology
Node Size	Small size preferred (no major limitation in most cases)	Miniaturization required
Node Accuracy	Accuracy outweighs a large number of nodes and allows for result validation	Each of the nodes has to be accurate and robust
Node Replacement	Easily performed (some nodes are disposable)	Difficulty in replacement of implanted nodes
Bio-compatibility	Not a concern in most applications	Essential for implants and some external sensors
Power Supply and Battery	Accessible, Capable of changing more frequently and easily	Difficulty in replacement and accessibility of implanted settings
Node Lifetime	Several years / months / weeks	Several years / months (application-dependant)
Power Demand	Power is more easily supplied, hence apparently greater	Energy supply is more difficult hence apparently lower
Energy Scavenging	Wind and Solar power are most apparent candidates	Thermal and Motion are most apparent candidates
Data Rate	More frequently homogenous	More frequently heterogenous
Data Loss Impact	Data loss over wireless transfer is compensated by a large number of nodes	Data loss is considered more significant (may need additional measures to assure real-time data interrogation capabilities and QoS)
Security Level	Lower (application-dependant)	Higher security level to protect patient information
Traffic	Application specific, Modest data rate, Cyclic/sporadic	Application specific, Modest data rate, Cyclic/sporadic
Wireless Technology	WLAN, GPRS, Zigbee, Bluetooth and RF	802.15.6, ZigBee, Bluetooth, UWB
Context Awareness	Insignificant with static sensors in a well-defined environment	Very significant due to sensitive context change of body physiology
Overall Design Goals	Self-operability, Cost optimisation, Energy Efficiency	Energy Efficiency, Eliminate electromagnetic exposure

2.4 Wireless Body Area Networks in Healthcare Applications

WBAN based health care applications use different biomedical sensors to provide continuous monitoring of patient health (Baba et al., 2018). The sensors in WBAN based health care applications are used to monitor vital parameters of a patient, such as cardiac activity (ECG), arterial oxygen saturation (SPO2), heart rate (BPM) and breathing. All data collected from the sensors is transmitted to a central node. This central node is connected to a computer which displays the data using a graphical interface. A patient’s health is monitored in real time as data collection, processing, and transmission happen in real-time. Hadjem et al. (2013) present a WBAN based healthcare application which enables the early detection of myocardial infarction for cardiovascular diseases using an electrocardiogram sensor.

Wearable sensor nodes which harvest solar energy enable the implementation of an autonomous WBAN based healthcare application. Wu et al. (2017) propose a WBAN based application using different wearable sensors such as an accelerometer, temperature and pulse sensors which are placed on different parts of the body. These sensors measure physical signals such as temperature and heartbeat. They can also detect falls using the node’s accelerometer and notify of an emergency situation. Similarly, Bhattacharya *et al.*(2016) propose a WBAN based distributed posture recognition application which consists of three tri-axial accelerometers. These accelerometers are worn on the thighbone, trunk, and shinbone respectively. The proposed solution helps to detect patient falls by differentiating between the static and dynamic postures. Salman et al. (2013) present a WBAN based application using a non-invasive lung monitor sensor which detects and diagnoses lung disease early. Traditionally, X-ray and CT scans have been used for diagnosing abnormalities in the lung. By analysing the data collected from the lung sensor, potential abnormalities of the dielectric constant of the underlying lung tissue are identified.

WBAN based applications can be very useful in helping disabled or blind people in their daily life. Choi et al. (2008) discussed how attaching a camera to eyeglasses and adding a sensor in an assistance stick can be useful in assisting blind people. By analysing the collected blips and images, a portable signal processor can convert this data to voice which is helpful for blind people. Additionally, a disabled person who is unable to speak or read can convert body motion to voice by attaching a sensor to their finger. Kavitha and Perumalraja (2014) present a WBAN based real-time healthcare application which monitors a driver's health condition by using various sensors to periodically collect physiological data such as pulse rate, breathing rate, temperature and blood pressure. If there is any abnormality found in the driver's health status, a smartphone-based application will send current health data to both a transport office and a healthcare provider using the cellular network.

2.5 Challenges for Wireless Body Area Network Applications

The main design requirements for any WBAN application is that the body sensor node needs to be extremely small and thin, capable of wireless communication, and use minimal power for data collection and processing (Antonescu and Basagni, 2013). User requirements such as privacy, safety, ease of use, security and compatibility are also of great importance (Salayma, Al-dubai and Romdhani, 2017). This section will detail the most challenging issues related to the development of a WBAN based healthcare application.

Energy efficiency

WBAN devices require an efficient energy source for data collection, processing and transmission, with data transmission likely to consume the most energy (Latré *et al.*, 2011). Most sensor devices in WBAN applications are powered by batteries. In some cases, such as sensors implanted in the human body, these batteries are not replaceable (Barakah and Ammad-Uddin, 2012). In WBAN applications, the power required by the sensor node can vary, depending on the application type and the communication medium. Therefore, it is essential to design an ultra-low powered radio transceiver which does not downgrade the reliability of the communication (Salayma, Al-dubai and Romdhani, 2017). If the application requires a high data transmission rate, an energy efficient data compression algorithm and transceiver needs to be used to reduce the number of bits. Reducing the number of bits helps to reduce the power consumption for data transmission (Chin *et al.*, 2012).

Antenna Design

To assure the reliability of the communication in a WBAN application, a suitable antenna design is a key element. Designing a suitable antenna is difficult due to factors such as the weight, posture and the type of skin of the person wearing the sensor node (Antonescu and Basagni, 2013). The size and shape of the antenna can be changed based on location in the body where it is worn. As the human body is considered a large inhomogeneous object with high permittivity, electromagnetic interaction between the human body and the antenna affects the properties of the antenna (S Movassaghi *et al.*, 2014).

Quality of service (QoS)

In a WBAN application, sensor nodes need to communicate with each other or with a personal handheld device. This means that communication channels can be heavily attenuated and shadowed by the human body. To preserve the quality of service (QoS), techniques including adaptive channel coding, dynamic power adjustment, and QoS-aware Media Access Control (MAC) need to be considered when designing the application (Antonescu and Basagni, 2013). WBAN applications demand a high degree of sensor data reliability in order to provide a quality patient monitoring service. Reliability of the data can be measured by the quality of the link or by the efficiency of end-to-end communication. To assure data reliability, a WBAN system needs to be fault tolerant and have a minimum quality of service (Salayma, Al-dubai and Romdhani, 2017). Assuring a reliable QoS means that all packets arrive on time and in their correct order. To achieve this, the system needs to have a mechanism to avoid or manage traffic congestion. Cavallari et al. (2014) discusses the need to implement appropriate error correction and interference-avoidance methods in the physical layer. This helps to reduce the bit error rate and end-to-end delay in communication and provide a higher-level QoS.

Security and privacy

Data security and privacy of patient's health records are two essential components for WBAN applications. Data security means assuring that data is protected from unauthorised users while the data is being collected, processed, stored and transmitted. Data privacy confers a right for individuals to control the collection and use of personal health information (Ramli and Ahmad, 2011). In a WBAN application, communication of patient health-related information needs to be private, confidential and unaltered while collecting the data from a sensor or sending it over to the internet to a server. It is also necessary to use an appropriate encryption technique to protect data from being tampered with or leaked (Barakah and Ammad-Uddin, 2012). Due to the resource constraints in terms of power, memory and computational capability, the security specifications and solutions proposed for other networks do not apply to WBAN applications (Samaneh Movassaghi *et al.*, 2014). It is necessary to implement controls that guarantee the confidentiality, integrity, availability and privacy of patient health record data in WBAN based healthcare applications. As complex mechanisms require more computation and power resources, it is necessary to have a solution that minimises both (Chin *et al.*, 2012).

2.6 Security and Privacy Requirements and Attacks for WBAN Applications

Due to the advancement in technology and the increasing popularity of healthcare-based applications, WBAN applications are one of the primary targets for security breaches and cyber threats. A WBAN security breach costs money and can create a life-threatening event in some cases (Kotz, 2011). So, proper safeguards need to be considered to protect the security and privacy of the WBAN based healthcare applications. To develop the safeguards, we first need to identify the list of attacks and security and privacy requirements. A list of attacks and security and privacy requirements unearthed during the literature review is now presented, along with a brief note on how these attack types and security and privacy requirements could affect a WBAN application.

2.6.1 WBAN Application Attack Types

Sensor nodes operate in an environment where many people have open internet access, therefore WBAN applications are vulnerable and open to many types of attacks and threats. Open connectivity creates a large attack surface. Additionally, WBAN applications are vulnerable to many types of attacks and threats as sensor nodes operate in an environment where the sensor node uses low powered radio signals for communication. These attacks make security and privacy of PHR data one of the primary challenges for WBAN systems. Attacks can also affect the performance and availability of the service, sometimes leading to life threating situations or even death (Kotz, 2011). Table 2-3 presents a list of attacks and a description of the attack found during the literature review.

Table 2-3: Types of attacks for WBAN applications in current literature

Types of attacks	Description
Denial-of-service (DoS)	As WBAN applications use different low-frequency wireless mediums including Bluetooth and ZigBee for communication, an attacker can transmit noisy signals to interfere with an actual radio signal of a wireless network to drop the traffic (Partala *et al.*, 2013). This attack can lead to unavailability of the service for other sensor nodes in the network with respect to channel access (Omoogun *et al.*, 2017).
Eavesdropping	An attacker can collect information along with personal health data by intercepting communications between the sensor node and the base station. This information can be used to break the key exchange technique during the pairing phase between the sensor node and the smartphone (Seneviratne *et al.*, 2017). By analysing data collected by eavesdropping, an attacker can introduce themselves as an authorised member of the network and launch an impersonation attack (Kompara and Hölbl, 2018).
Man-in-the-middle	An attacker can place himself as a relay or proxy into a communication session between two entities. The attacker can eavesdrop and manipulate the message in real-time without the sender or receiver noticing. In this case, the sender and receiver will presume that they are communicating directly to each other (Kompara and Hölbl, 2018).
Insider attack	In WBAN applications an attacker can launch an insider attack by using a physically compromised node with authorised system access. As an authorised node is familiar with the network and application security policy, the attacker will get distinct advantages over external attackers. Using an insider attack, an attacker can drop, modify and misroute data packets to harm normal network functionality (Alsadhan and Khan, 2013).
Sniffing attack	In WBAN applications an attacker can place an adversary node in the network to intercept or listen to the wireless communication channel. Due to wireless networks being a less secure and shared medium, if data packets are not encrypted, they can be read using network sniffing tools (DEMİR and TATLI, 2018). An outside attacker can retrieve vital information including source address, destination address, port and protocol type from network data packets (Langone, Setola and Lopez, 2017).
Physical attack / node-compromising attack	As sensor nodes of a wearable WBAN application are placed on the body, a node can be easily physically tampered with as they are not tamper proof (Li, Lou and Ren, 2010). By injecting malicious code, an attacker can alter the information or re-engineer the system. This altered health-related data may result in a patient's death. Additionally, having physical access to the node, an

Types of attacks	Description
	attacker can extract all data including the cryptographic key or sensitive health information from the sensor node (Al-Janabi *et al.*, 2017).
Sinkhole attack	In WBAN applications a compromised node can advertise itself as a best possible route to the base station to its neighbouring nodes. Using the compromised node, the attacker can also drop or redirect all collected packets which will never reach their destination (Kompara and Hölbl, 2018).
Masquerading attack	In a WBAN application an attacker can impersonate or clone an authenticating device to launch a masquerading attack. By using this attack, an attacker can use this masquerade node to steal data, inject false information or get full access to the healthcare application. With full access to the application, the attacker can modify or delete PHR data from the medical database (Sherali Zeadally, Jesús Téllez Isaac, 2016).
Spoofing and Sybil attack	A spoofing attack is when a malicious node masquerades as another legitimate entity of the system to disrupt the network while avoiding detection. In WBAN applications this attack also facilitates the larger Sybil attack where identities of multiple nodes in the network are compromised. In a Sybil attack, a single malicious entity can also present itself with multiple identities (Bharathi and Venkateswari, 2018).
Data falsification / Data modification	An attacker can perform unauthorised modification of data packets to falsify the information transmitted in the network by placing a compromised node nearby. In WBAN applications, this modified information can trigger a false alarm or send unnecessary responses (Thamilarasu and Odesile, 2016).
Replay attack	In the WBAN application scenario, the attacker can collect sensitive health information and continuously retransmit to trick the receiver into gaining credentials or to cause confusion and errors in the system. It can harm the patient by continuously sending old health information, which can prevent the system from detecting a critical situation (Alsadhan and Khan, 2013).

The literature indicates that the most referenced attacks for WBAN applications are DoS (120 papers), eavesdropping (114 papers), replay attacks (106 papers), data falsification (103 papers), and physical attacks (55 papers). The least referenced attacks are insider attack (13 papers) and sniffing attack (9 papers). An attacker could make applications unavailable by launching a DoS attack and this can cause life-threating events. Eavesdropping attacks can be utilised to collect PHR data and cryptographic information which will compromise the privacy of the user. The number of attack types for WBAN applications referenced in the literature gradually increased from five in 2008 to eleven in 2021. A detailed analysis of eavesdropping attacks based on occurrences for WBAN applications from 2008 to 2021 is presented in Figure 2-4. The chart illustrates a steady increase in the number of papers reporting eavesdropping attacks from 2008 (2 papers) to 2017 (14 papers). However, 2018 indicates a major increase in the number of papers reporting eavesdropping attacks (32 papers). While this literature review extended to the first quarter of 2021, the growth is similar to 2020. Masquerading attack and physical / node compromise attack were added to the list in 2009. By using a compromised node, an attacker can launch several other types of attack such as insider attack, sinkhole attack, and replay attack. It is necessary to take countermeasures to make each sensor node tamper-proof.

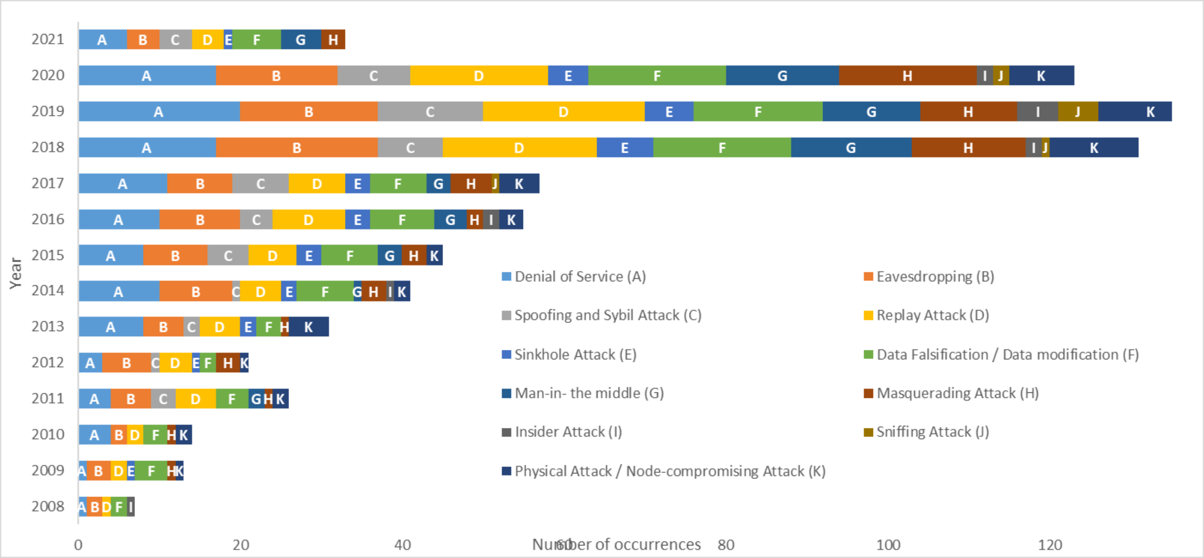


Figure 2-4: Attack landscape based on occurrences for WBAN applications throughout 2008-2021

For the period of this literature review, spoofing attacks were introduced in 2011. Between 2015 and 2020 the number of references to spoofing attacks has steadily increased. Due to recent developments of various tools for extracting device identity and localisation information, attackers can use this information to launch spoofing attacks. Although sniffing attacks are a widely known attack in the context of network security, very few authors have addressed these attacks for WBAN applications. In a WBAN application, an attacker can use popular sniffing tools such as Wireshark and Fiddler to capture data packets over the network. By analysing these data packets attackers can gain details about the communication protocol and the nature of the data.

2.6.2 Security and Privacy Requirements for WBAN Applications

The security and privacy of health-related data is one of the primary challenges of WBAN systems. The data confidentiality, integrity and availability (CIA) triad is a common concept to assure data security. Confidentiality assures that data is not made available or disclosed to unauthorised individuals or entities. Integrity provides assurance that data is not modified accidentally or deliberately, safeguarding the accuracy of the data. Availability assures the reliable accessibility of the system for authorised entities. Data privacy governs how data is collected, shared and used; it also assures that only authorised persons can access the data. However, data privacy cannot be achieved by securing only personally identifiable information (PII). As PHR data includes both PII and patient health record data, so privacy needs to be assured for both PII and health record data. According to the NISTIR 8062 standard, privacy concerns can arise from intentional or authorised processing of PII data. Figure 2-5 details the relationship between information security and privacy.

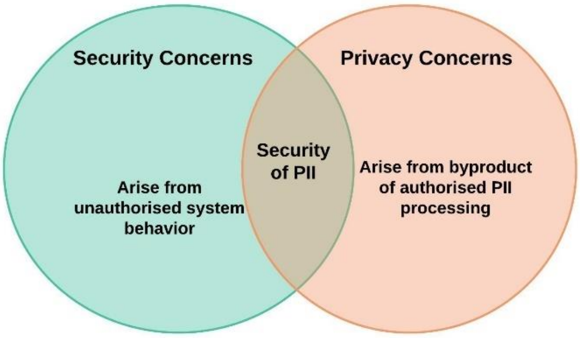

Security Concerns
Privacy Concerns
Security of PII
Arise from unauthorised system behavior
Arise from byproduct of authorised PII processing

Figure 2-5: Relationship Between Information Security and Privacy (NISTIR 8062)

The literature review conducted as part of this research unearthed 22 security and privacy requirements. A description of these 22 security and privacy requirements and their relevance to WBAN applications is presented in Table 2-4.

Table 2-4: List of security and privacy requirements with a description for WBAN applications

Security and Privacy Requirements	Description
Data Confidentiality	Since WBAN healthcare applications contain sensor nodes that store and transmit sensitive health information, data confidentiality is one of the most important challenges (Ramli and Ahmad, 2011). Li et al. (2010) state that PHR data needs to be protected from unauthorised access and leaking while in storage in a sensor node or local server.
Data Integrity	As data confidentiality does not protect data from external modifications, data integrity is needed. Data integrity provides assurances that data is not modified during transmission or while in storage (Dodangeh and Jahangir, 2018). As WBAN based healtcare applications contain sensitive patient medical information, a patient's life could be in danger without the protection of data integrity. For example, in a healthcare application scenario, a little modification to a laboratory report or prescription can lead to the wrong medication being prescribed by a doctor (Sajid and Abbas, 2016)
Authentication	In WBAN applications the authentication process will check the identity of a user before allowing the user to access any PHR data. Al-Janabi et al. (2017) state that WBAN network senders and receivers need to calculate a Message Authentication Code for all the data before transmission. Using this code allows both entities to assure that the message is from a trustworthy source. Additionally, both the sender and receiver in the network can authenticate each other by a mutual-authentication

Security and Privacy Requirements	**Description**
	technique before sharing any data. This helps to mitigate man-in-middle attacks (Kompara and Hölbl, 2018)
Non-repudiation	To preserve the privacy of the PHR data in WBAN, the application needs to have the ability to assure that an entity cannot deny the authenticity of a message which originated from it. While the system is accessed by an authenticated user, it is necessary to keep a constant check on the activity of that authenticated user. The entity will be unable to deny that it made certain changes (Sajid and Abbas, 2016).
Access Control	Access control is also a growing concern for maintaining the privacy of healthcare data in WBAN applications due to the sensitivity of the information. Sajid et al. (2016) state that it is necessary to define a fine-grained access control policy in WBAN applications to assure that PHR data will not be accessed by an unauthorised entity. Li et al. (2010) present a WBAN application scenario where PHR data may be accessible by doctors, medical staff, pharmacists and other service agencies. If an insurance company got access to patient health information, they might offer higher health insurance premiums to that patient. Therefore, a fine-grained access policy needs to enforce different access privileges to users.
Availability	In WBAN applications, data availability assures data is available to the application or authorised entities whenever it is required. An attacker may target the service by launching DoS attacks to make the application inaccessible or flood the network with traffic to make it unavailable (Kyaw and Cusack, 2014). In a medical emergency, the unavailability of the network means doctors will be unable to access PHR data, which may lead to loss of life of a patient. So, assuring data availability must always be a high priority in all healthcare systems (Naik and Samundiswary, 2016).
Data Privacy	Data privacy assures that only authorised persons can access the data. In WBAN applications data privacy is a major concern as sensor nodes collect, process and transmit health-related data. It is necessary to assure that this health-related data is not leaked to unauthorised persons (He et al., 2017). According to Ara et al. (2017), data privacy is a major challenge due to resource constraints within WBAN based remote health monitoring services, as disclosure of sensor data will violate data privacy.
Encryption/ Cryptography	As WBAN sensor nodes have limited processing power, memory and energy constraints, data encryption is a key challenge. With the help of lightweight and energy-efficient cryptography algorithms, data will be converted into a human unreadable format while it resides in storage (Cavallari et al., 2014). By using symmetric and asymmetric cryptography algorithms, user-health data can be encrypted. Data Encryption Standard, Advance Data Encryption Standard, Elliptic Curve Cryptography, and the Rivest Shamir Algorithm are some widely used cryptographic algorithms (Sawaneh, Sankoh and Koroma, 2017).
Key Management	In WBAN applications, key management is constrained by sensors computational power, battery power, memory and transmission range. Masdari et al. (2017) present the operations of a key management service as key generation, key refreshing, key agreement, key distribution and key revocation. Generating unique cryptographic keys is the most important challenge to assure data security. Similarly, key revocation and renewal processes need to be in place to revoke a compromised cryptographic key.
Data Freshness	Data freshness is an important factor in assuring data integrity and confidentially in WBAN applications. It assures that data packets are in the correct format and not previously used (Naik and Samundiswary, 2016). Sawaneh et al. (2017) present two types of data freshness techniques currently in use: strong freshness and weak freshness. Strong freshness is required when a sensor node is performing a synchronisation process with the coordinator or a personal server as it provides a guarantee of time delay with data packet frame ordering. Weak freshness is required when the sensor node is working with a low-duty cycle pulse, as it will not require any guarantee of time delay (Al-Janabi et al., 2017).
Firewall	In WBAN applications firewalls can be used as the first line of defence to protect sensitive information. Omoogun et al. (2017) discuss the use of firewalls and specific access control lists that protect WBAN applications from different attacks such as DoS attacks. They also state that firewalls can also restrict malicious users from gaining access to the application.
Accountability	Accountability is the process of identifying unauthorised actions and holding users accountable for their actions (Ramli and Ahmad, 2011). In WBAN based applications, healthcare providers need to safeguard PHR data by making the user (both authorised and unauthorised) accountable for their actions (Al-Janabi et al., 2017). Similarly, to assure data privacy in a healthcare system, it is necessary to identify dishonest users (both authorised and unauthorised) and make them accountable for their actions (Sajid and Abbas, 2016).
Revocability	In WBAN applications it is necessary to have a process to revoke a user's privileges or to revoke a sensor node as soon as they are identified as compromised or behave maliciously (Dodangeh and Jahangir, 2018). As the number of users and sensor nodes can be large in a WBAN application, a fine-grained revocation process needs to be implemented to revoke one or many entities from a system. During this revocation process, it might require updating a compromised user or node's secret key by using broadcast messages (Li, Lou and Ren, 2010).

Security and Privacy Requirements	Description
Intrusion Detection	An intrusion detection system is a set of techniques or methods to identify and block suspicious activity in a network or host (Al-Janabi et al., 2017). Thamilarasu et al. (2016) present two types of intrusion detection system that can be used for a WBAN application, 1) Rule-based detection and 2) Anomaly-based detection. Rule-based detection techniques use a signature database to evaluate network and host activities against pre-defined attack patterns and signatures. Anomaly-based detection uses profile-based techniques, which evaluate network or host activities against pre-defined behaviour profiles. If any inconsistencies are found during the evaluation process, it will be reported as an anomaly.
Trust Management	In a WBAN based healthcare application trust management needs to take place in a real-time setting to provide trustworthiness between sensor nodes to provide a tamper-proof and efficient service (Al-Janabi et al., 2017). It is also essential to verify that data originates from a trusted sensor and not from an attacker (Saleem, Ullah and Kwak, 2010). Without a trust-based solution in place, cryptographic solutions can become ineffective or useless against an internally compromised node (Thamilarasu and Odesile, 2016).
Forward secrecy / Backward secrecy	To preserve data confidentiality and privacy in WBAN applications it is necessary to assure that an attacker can not trace any data by collecting information from previous and future communication. Proper key management and cryptographic techniques with forward and backward secrecy are needed to preserve data confidentiality and privacy (Challa et al., 2018).
Resilience	In WBAN applications resilience is defined as how capable the system is in resisting external and internal failures and how fast the system can recover from a failure state to a stable state. Salayma et al. (2017) state that designing an efficient and resilient WBAN application is challenging due to the diversity of sensor nodes and dynamic environments. Current ongoing research mostly focuses on mitigating technical issues such as mobility and sensor design, but designing fault detection and system recovery in WBAN applications are still at an early stage of development.
Physical Protection	In WBAN applications it is necessary to assure physical protection for all sensor nodes, mobile devices and medical backend data servers. Singel et al. (2008) listed the medical backend data server as one of the most security-critical devices in a WBAN application. The backend server is used to collect and store PHR data from all the sensor nodes. It is necessary to assure physical security by implementing appropriate access controls.
Auditability	Auditability is one of the least addressed requirements for assuring data security and privacy in a healthcare application (Sajid and Abbas, 2016). In a medical emergency scenario, patients using a WBAN application might not be convinced to grant access to their health-related data due to mistrust of the Emergency Medical Care (EMC) provider. It is necessary to keep track of access activities of PHR data even if it is by an authorised entity (Sajid and Abbas, 2016). If EMC providers try to misuse the PHR data, it can be tracked through auditing.
Client Platform Security	Usually, in WBAN applications sensor nodes send data to a personal handheld device which is used for storing or processing data. Sajid et al. (2016) discuss how very limited work has been done on assuring data security and privacy of the software and hardware used by end-users in healthcare applications. The end-user system includes mobile devices, personal computers and networks. If these end-user systems are comprised by an attacker, the privacy of stored PHR data may be jeopardised, or it may leave the system open to attacks. Therefore, it is necessary to assure data security and privacy on these end-user systems.
Anonymity	Anonymisation is a process which aims to prevent identification of the individual with whom data is related. For a WBAN application, it is necessary to assure that an adversary cannot trace any user by collecting sensor data (Dhillon and Kalra, 2018). Similarly, in Sajid et al. (2016) state that anonymisation can be used to assure data security and privacy of the user in WBAN applications by hiding the patient's key identification information. The anonymised data will protect users' privacy as a particular individual will not be able to be linked or associated with the data during the data retrieval or the data storage processes.
Regulations and compliance requirement	Assuring the security and privacy of PHR data has become a global concern. To preserve data privacy, there are different sets of regulations or rules available all over the world. Among them, the two most important are the American Health Insurance Portability and Accountability Act for the US region and the General Data Protection Regulation for the EU region. It is necessary to implement sets of rules or policies in WBAN applications to assure access to patient health-related data which will protect the patient's privacy (Al-Janabi et al., 2017). In both cases, the regulatory compliance bodies provide a set of rules for doctors, healthcare providers and hospitals to assure data privacy and security of PHR data. If any healthcare service provider fails to meet the rules and a data breach happens, the service provider can face civil or criminal consequences, including fines.

As discussed earlier in this section, the CIA triad along with privacy is required for assuring data security and preserving the privacy of PII and PHR data in WBAN based healthcare applications. Table 2-4 shows that to assure data security and privacy in WBAN applications, other security and privacy requirements need to be taken into account, such as proper access control, key management and lightweight cryptography algorithms. Some of the security and privacy requirements help to assure multiple properties of the CIA triad and privacy. For example, proper access control will help to assure data confidentiality and privacy while key management and lightweight cryptographic techniques will protect data confidentiality and integrity. Implementing the correct client platform security measures will assure data confidentially, integrity, availability and privacy.

One of the goals of this research is to survey the security and privacy requirements landscape for WBAN based healthcare applications. During the literature review process, a total of 22 security and privacy requirements were identified which are required to assure data security and privacy of WBAN based healthcare applications. As Table 2-5 indicates, the security and privacy requirements were recorded in an excel spreadsheet along with the research paper ID. This table is a snapshot showing just fifty papers. The full table is available in Appendix A. This list of security and privacy requirements will help to develop a data security and privacy framework for WBAN applications.

Table 2-5: Mapping of occurrence of security and privacy requirements for WBAN applications in current literature

Ref no	**Data Confidentiality**	**Data Integrity**	**Authentication**	**Non-repudiation**	**Access Control**	**Availability**	**Privacy**	**Encryption/ Cryptography**	**Key Management**	**Data Freshness**	**Firewall**	**Accountability**	**Revocability**	**Intrusion Detection**	**Trust Management**	**Forward secrecy / Backward secrecy**	**Resilience**	**Physical Protection**	**Auditability**	**Client Platform Security**	**Anonymity**	**Regulations and compliance requirement**
P1	x	x	x	x	x	x						x	x									
P2	x	x	x			x	x		x	x				x	x		x					
P3	x	x				x																
P4		x	x		x			x			x											
P5	x	x	x			x								x	x							
P6	x	x	x	x	x	x	x	x	x	x				x								
P7	x	x				x																
P8	x	x			x					x												
P9	x	x							x	x												
P10	x		x				x	x														
P11	x	x	x			x			x	x		x		x	x							x
P12	x	x	x	x	x	x	x					x	x									
P13	x	x	x			x	x	x	x	x												
P14	x	x	x	x	x	x	x	x	x	x		x										
P15	x	x	x	x		x	x			x			x			x					x	
P16	x	x	x	x	x		x	x				x							x	x	x	
P17	x	x	x			x																
P18	x	x	x	x			x		x							x						
P19	x	x	x				x	x														

Ref no	Data Confidentiality	Data Integrity	Authentication	Non-repudiation	Access Control	Availability	Privacy	Encryption/ Cryptography	Key Management	Data Freshness	Firewall	Accountability	Revocability	Intrusion Detection	Trust Management	Forward secrecy / Backward secrecy	Resilience	Physical Protection	Auditability	Client Platform Security	Anonymity	Regulations and compliance requirement
P20	x	x	x	x	x	x	x	x	x	x												
P21	x	x	x						x							x						
P22			x		x				x									x				
P23	x	x	x			x										x					x	
P24	x	x	x	x	x	x	x															
P25			x																			
P26	x	x	x			x			x	x												
P27	x	x	x		x																	
P28	x	x	x	x	x																	
P29			x		x			x	x													
P30	x	x	x	x	x	x				x							x					
P31	x	x	x	x	x	x						x	x									
P32	x	x				x																
P33	x	x	x	x																		
P34			x			x	x															
P35	x	x				x	x															
P36		x	x					x		x												
P37	x	x	x		x	x		x	x	x					x		x					
P38	x	x	x																			
P39	x	x	x							x												
P40	x	x	x				x															
P41	x	x	x						x								x				x	
P42	x	x	x			x	x		x	x												
P43	x	x	x		x	x	x	x	x			x										
P44	x	x	x	x			x	x	x							x					x	
P45		x					x															
P46		x	x				x	x		x												
P47	x	x	x			x			x	x												
P48			x				x	x														
P49		x	x				x	x		x												
P50	x	x	x		x			x				x							x		x	

The literature indicates that the most referenced WBAN security and privacy requirements are data confidentially (186 papers), data integrity (181 papers), authentication (186 papers), encryption (139 papers), data privacy (138 papers), data availability (97 papers), key management (93 papers) and access control (76 papers). Authentication with fine-grained access control is required for assuring data confidentiality and privacy (Ragesh and Baskaran, 2012). Lightweight cryptographic techniques can be used in memory and computational power-constrained systems to assure data integrity and confidentially (Mohd, Hayajneh and Vasilakos, 2015). To achieve data integrity using a cryptographic technique, a proper key management process with forward and backward secrecy support is also required (Masdari, Ahmadzadeh and Bidaki, 2017).

The least addressed security and privacy requirements are a firewall, physical protection, auditing, client platform security, and anonymity. Omoogun et al. (2017) states that to assure data availability in WBAN applications, it is necessary to have a firewall and intrusion detection system in place so that the application can take the necessary prevention and detection actions against different types of attack. Furthermore, in WBAN based healthcare applications, it is necessary to assure data privacy by adopting guidelines provided by regulatory bodies (Al-Janabi *et al.*, 2017).

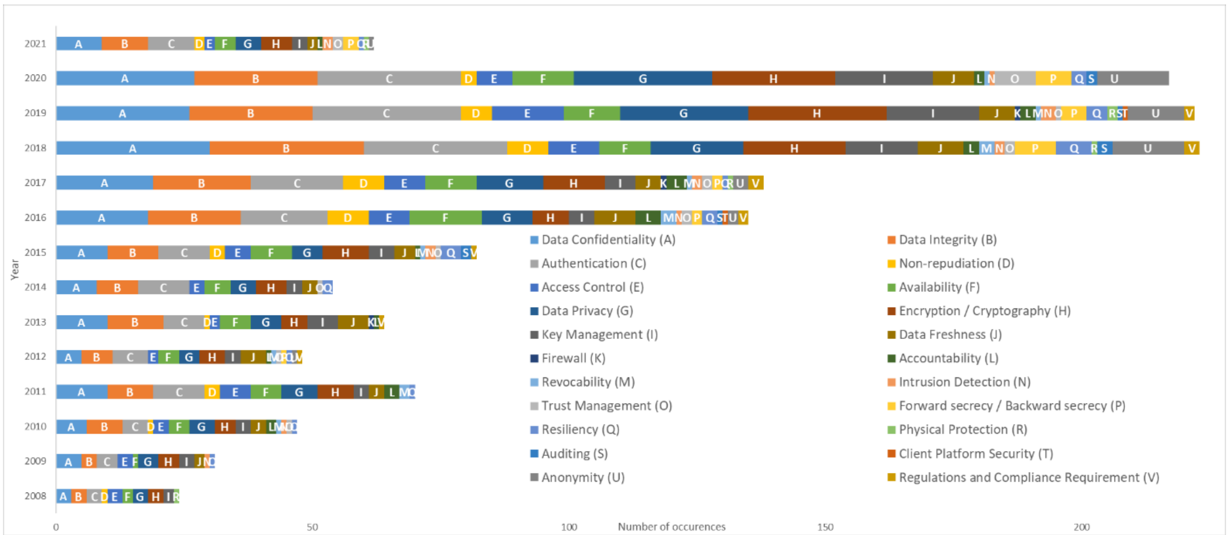


Figure 2-6: Security and privacy requirements landscape based on occurrences for WBAN applications throughout 2008-2021

To view how security and privacy requirements for WBAN based healthcare applications have changed from 2008 to 2021, a stacked graph was created. This graph was created by using the number of occurrences of each security requirement each year. Figure 2-6 presents security and privacy requirements by year from 2008 to 2021. It can be seen that the number of security and privacy requirements increased from 10 in 2008 to 22 in 2021. The chart illustrates a steady increase in the number of papers reporting requirements from 2008 (3 papers) to 2020 (32 papers). While this literature review extended to the first quarter of 2021, the growth is similar to 2020. Among them confidentiality, integrity and authentication have the highest occurrences each year. Due to easy access to apps installed on mobile devices, auditing, client platform security and anonymity have appeared from 2015 onwards. As security and privacy of PHR data has become a global concern, regulatory compliance requirements for WBAN applications started having a presence from 2012 onwards.

2.7 Existing Approaches for Addressing Security and Privacy Requirements and Attacks

Substantial research has been conducted into data confidentially, integrity, availability, authentication and privacy of WBAN based healthcare applications. In this section, we present a detailed overview of the existing frameworks or solution approaches and note their limitations in addressing the security and privacy requirements detailed in the previous section. During the review process, each framework or solution approach was analysed to determine the security and privacy requirements for which they provide countermeasures. Table 2-6 presents a mapping of existing frameworks or solution approaches to the security and privacy requirements presented in section 2.6.2. In most cases, the approaches provide a countermeasure for multiple security and privacy requirements.

Table 2-6: Mapping of framework or solution approach with security and privacy requirements for WBAN applications

Refference	Data Confidentiality	Data Integrity	Availability	Authentication	Anonymity	Non-repudiation	Forward Secrecy / Backward Secrecy	Key management	Accountability	Auditability	Access Control	Encryption/ Cryptography	Resilience	Privacy	Revocability	Data Freshness	Intrusion detection	Firewall	Trust Management	Physical Protection	Client Platform Security	Regulations and compliance requirement
Liu *et al.* (2014)				x	x	x		x				x		x								
Li et al. (2016)	x	x		x		x	x	x		x	x	x		x	x							
Ramli et al. (2013)	x	x		x				x				x										
Mantas et al. (2009)		x										x										
Odesile et al. (2017)													x				x					
Han et al. (2014)	x	x		x				x				x		x		x						
Yin et al. (2017)	x	x		x							x	x										
Alsadhan et al. (2013)	x	x						x								x						
Sridharan et al. (2014)	x	x		x				x				x										
Hussien et al. (2016)				x				x				x										
Alshamsi et al.(2017)												x										
He et al.(2014)	x	x		x								x				x						
G. Thamilarasu (2015)																	x					
Wang et al.(2018)				x								x										
Thampi et al.(2015)												x										
Das et al.(2017)				x																		
Sridharan et al.(2013)				x				x				x										
Iqba et al. (2013)	x	x		x			x															
Andrew et al. (2018)	x	x		x	x	x																
Wu et al. (2016)				x	x		x	x														

Refference	Data Confidentiality	Data Integrity	Availability	Authentication	Anonymity	Non-repudiation	Forward Secrecy / Backward Secrecy	Key management	Accountability	Auditability	Access Control	Encryption/ Cryptography	Resilience	Privacy	Revocability	Data Freshness	Intrusion detection	Firewall	Trust Management	Physical Protection	Client Platform Security	Regulations and compliance requirement
Al-saleem et al.(2017)				x				x														
Cagalaban et al.(2012)	x		x	x				x			x	x										
Ramu (2018)	x	x		x																		
Abdmeziem et al.(2014)	x	x		x				x				x										
Dhillon et al.(2018)	x	x	x	x	x		x	x														
Zhou et al.(2013)								x				x										
Ragesh et al.(2012)	x	x		x		x					x	x		x	x							
Sarvabhatla et al.(2015)				x	x		x															
Li et al.(2013)							x	x														
Gebrie et al.(2017)	x	x		x		x								x								
Sampangi (2014)		x		x		x		x				x										
Huang et al.(2016)				x				x														
Shankar et al.(2015)				x				x				x		x								
Shen et al.(2018)	x	x		x	x	x	x	x														
Dodangeh et al.(2018)	x	x		x			x	x				x				x						
Wu (2014)				x							x								x			
Li et al.(2015)																			x			
Zhou et al.(2015)	x	x						x				x		x								

Liu et al. (2014) developed two certificate-less remote anonymous authentication schemes as a certificate-less cryptography (CLC) primitive by carefully exploring the special characteristics of WBANs. The proposed solution addressed a total of 6 from 22 security and privacy requirements. The CLC still requires a trusted third-party key generating centre (KGC) which will produce a partial private key using a master key and a user's identity. Since the KGC does not possess the secret value, it does not know the full private key. The advantage of this scheme is that there will be no key escrow problem nor issue with the public key certificate. The preliminary version of the authentication scheme cannot provide anonymity since a constant value related to user identity is transmitted. The security-enhanced version of the authentication scheme is also vulnerable to the identity threat or masquerading attack since every application provider should maintain an identity verifier table. Li et al. (2016) design an efficient certificate-less signcryption access control scheme based on CLC which addressed a total of 11 from 22 security requirments. This modified version of the access control scheme can be used to authorise, authenticate, and revoke user access to WBANs. This scheme helps to achieve confidentiality, integrity, authentication, non-repudiation, public verifiability, and ciphertext authenticity.

Ramli et al. (2013) suggest a biometric-based security framework model for data authentication in WBAN applications which addressed 5 from 22 security and privacy requirements. This method uses user vital signs such as ECG data to generate cryptographic keys for sensors to secure the communication and encryption and decryption of the message. This scheme also uses the Message Authentication Protocol as a key for authentication between source and destination and omits complex key generation methods for implementing authentication in WBANs. The authors did not present any discussion about energy and power efficiency of the scheme. No authentication protocol was presented in the framework.

Han et al. (2014) proposed a Multi-valued and Ambiguous Scheme (MAS) to secure communication between the cloud and WBAN’s in healthcare systems. This scheme mainly deals with data confidentiality and provides a general paradigm for deploying applications in Cloud-assisted WBANs. The author also proposed a new method to design cryptosystems as the standard approach to protect data. In this new method, users can encode data with a secret key that can only be decoded by the intended receivers. The proposed scheme uses Dijkstra’s cryptographic algorithm with the concept of multi-value rules for encoding to assure the patient’s data confidentiality. However, as Dijkstra’s algorithm is not time efficient, this scheme would have high overhead in terms of encryption and decryption.

Sridharan et al. (2014) proposed a Data Authentication Model (DAM) to achieve confidentiality and authenticity with the help of a private key that is shared between both parties before the message transfer. In this proposed DAM model, authentication challenges are addressed specifically by using a simple shared private key technique instead of a complex cryptographic key distribution algorithm. This simple shared private key cryptographic technique will require less computation resources for encryption and decryption processes. It will save power utilization for the entire process of medical data transfer to the healthcare unit while adequate security measures are employed. In Alshamsi et al. (2016) the authors proposed a Lightweight Encryption Algorithm (LEA) as an efficient algorithm for WBAN applications. This adds a layer of encryption to patient vital signs captured by the sensor and sent to a mobile device that a patient carries. The authors also stated that LEA is more suitable than other cryptographic algorithms for WBAN environments, where the sensor devices have limited memory space and processing power.

Zhou et al. (2015) proposed a privacy preserving key management scheme for cloud-assisted WBAN applications. The authors used a blinding technique and embedded body sensors as key parts of the symmetric key establishment mechanism. In cryptography, blinding is a technique where service providers will provide service to a client in an encoded form without knowing real input and output. This techique will help to achieve the privacy of the patient's id, sensor deployment, and location. The proposed solution will also help to resist both time-based and location-based mobile attacks.

Odesile et al. (2017) proposed an intrusion detection system for WBANs using a distributed autonomous mobile agent, where every node in the network acts as the computing node, and mobile agents migrate and collaboratively perform attack detection. The proposed framework also uses machine learning algorithms to perform local and network level anomaly detection. Sensor agents can perform local detection using the attack features available in the limited sensing region, while gateway nodes and servers can perform global attack detection. The proposed solution is capable of identifying DoS and eavesdropping attacks.

A trust management scheme is required in WBAN applications to consider whether a node is trustworthy, reliable and secure while interacting with other sensor nodes. However, very few trust-based solutions have been proposed for WBAN applications. Li et al. (2015) proposed a lightweight trust system named BAN-Trust, which does not rely on any encryption technique and is easily deployable on commercial off-the-shelf sensor nodes. This approach uses collaborative filtering techniques based on the recommendation of neighbouring sensor nodes in a network. Each sensor node maintains a vector of its trust values and every neighbour's sensor node in the network. The sending node queries its neighbour's node about their opinions on the intended recipient and subsequently assign a weight to their opinions based on the level of similarity between the sender and the neighbour's trust vector's value. The sending node computes the trust of the receiver node by a weighted average of the individual opinions from its neighbour's nodes. If a new node is added or a neighbouring node cannot evaluate the node, the neighbouring node will weigh the node with a default rating. Once the default rating is received, the sending node will calculate the trust based on the default rating and the similarity of the new node with the existing node.

A blockchain is an advanced distributed ledger consisting of a series of blocks which are time slotted and connected through a crypto-graphic hash. This advanced distributed ledger can also be used to maintain and store transaction and activity data. In Zhang et al. (2019) the authors propose an efficient conditional identity privacy-preserving public auditing mechanism which checks the integrity of data hosted in the cloud server. The proposed auditing scheme assigns an anonymous id to each piece of patient data before storing into a cloud server which will preserve the privacy of the user data. The authors also integrate Ethereum blockchain to store the transaction data. The patients can anonymously use this transaction data to check whether privacy is comprised due to the malicious auditing behaviours.

In summary, Table 2-6 indicates that none of the approaches provide a countermeasure for all the security and privacy requirements listed in Section 2.6.2. The literature indicates that most of the security approaches provide for data confidentiality, integrity, authentication, key management and cryptographic techniques. Very few of the approaches address countermeasures for privacy, auditability, trust management, intrusion detection and resilience.

WBAN PHR data can be stored on client's mobile devices, however none of the existing security approaches provide any guidelines on how to achieve security for those mobile devices. As a WBAN based healthcare application processes patient PHR data, it is necessary to assure data security and privacy by adopting guidelines provided by different regulatory bodies. During the review process, it was noted that none of the authors discussed regulatory compliance requirements during the development of the security framework or solution approach.

2.8 Regulations and Standards

Security and privacy are key concerns for WBAN based healthcare applications due to the sensitive data they process, store and transmit. The implementation of effective security and privacy controls are important tasks which can have significant impact on the operations and budgets of an organisation. Country-specific rules and regulations also need to be taken into account during the implementation of security and privacy controls. This section presents a detailed description of widely used regulations from the USA and Europe followed by a review of international security and privacy standards.

2.8.1 Regulations

Healthcare applications and medical devices need to be compliant with various regulations. Assuring security and privacy is a vital requirement for compliance with regulations. This section presents the various regulations from the US and EU markets with their individual security and privacy requirements.

FDA

The 800 series under Title 21 of the Code of Federal Regulations (CFR) outlines the regulations which govern medical devices within the United States (US). These regulations are enforced by the Food and Drug Administration (FDA). The FDA recognises that the security and privacy of medical devices is a shared responsibility among stakeholders, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices (FDA, 2020). Medical devices should be designed to protect assets and functionality, and to reduce the risk of loss of authenticity, availability, integrity and confidentiality. As part of 'Title 21 CFR part 820 - Quality System Regulation' states that the medical device manufacturer needs to employ a cybersecurity risk management program (CFR, 2020). The aim of the risk management program is to reduce the likelihood of the device functionality being compromised, intentionally or unintentionally, by inadequate cybersecurity. An effective cybersecurity risk management program should address cybersecurity in both premarket and postmarket medical device development lifecycle phases.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was brought forward by the secretary of the US Department of Health and Human Services (HHS) as a law to enforce regulations for governing electronically managed patient information in the healthcare industry, and includes privacy and security protection of electronic personal health information (e-PHI) (HIPAA, 2020). Title II of HIPAA provides five rules: Privacy Rule, Transactions and Code Sets Rule, Security Rule, Unique Identifiers Rule, and Enforcement Rule. The purpose of these rules is to prevent fraud and abuse within the healthcare system. The Privacy Rule's objective is to guarantee that people's health information is appropriately secured while permitting the flow of information required to deliver and promote high-quality healthcare and safeguard the general public's health and well-being. The Privacy Rule requires different policies and procedures to provide federal protections for personal health information held by covered entities. This rule also assures patient rights concerning the authorisation, revoking consent, viewing their e-PHI, and asking for changes if their e-PHI is inaccurate or incomplete. The Security Rule specifies a series of administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of electronically protected health information. Below are the key security and privacy requirements outlined in the HIPAA Security and Privacy Rule:

- Assure the confidentiality, integrity, and availability of all e-PHI while created, received, stored and transmitted
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures of the information
- Perform risk analysis as part of the security management processes
- Implement technical policies and procedures that allow only authorised persons to access e-PHI
- Implement policies and procedures to assure that e-PHI is not improperly altered or destroyed
- Implement security measures to guard against unauthorised access to e-PHI

EU Medical Device Regulations

The European Medical Device Regulation (EU MDR) assures high standards of safety, security, and quality of medical devices being marketed within the EU for human use (EU Commission, 2017). The EU MDR is also known as EU Directive 2017/745 and 2017/746, was published in 2017. The cybersecurity requirements listed in Annex I of the MDR deal with premarket and postmarket aspects of medical devices. Below is the list of key cybersecurity requirements from the EU MDR:

- Manufacturers shall establish, implement, document and maintain a risk management system
- Medical device software should be developed in accordance with the state-of-the-art principles of the development life cycle, risk management, including information security, verification and validation

- Manufacturers shall set out minimum requirements concerning hardware, IT network security measures, including protection against unauthorised access
- Implement proper safeguards to avoid unauthorised access, disclosure, dissemination, alteration or loss of information and personal data processed
- Implement adequate safeguards to assure confidentiality of records and personal data of subjects
- Implement proper incident response plan and safeguards in case of a data security breach in order to mitigate the possible adverse effects

GDPR

The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for citizens in the European Union (EU) and European Economic Area (EU Commission, 2016). It was introduced in May 2018. The EU commission designed the GDPR to achieve the following key goals:

- Protect the rights, privacy and freedom of individuals in the EU
- Reduce the barrier for free movement of data inside the EU
- Inform individuals how personal data will be processed and who will get access
- Individuals will be able to obtain their data and reuse it for their own purposes
- Individuals have the right to restrict access and erase their data

GDPR will have a significant impact on the healthcare sector due to the volume and nature of sensitive personal data. This data is mainly used to provide patient care, real-time monitoring and for scientific research. Below is the list of key cybersecurity requirements of GDPR:

- Security measures must protect the confidentiality, integrity, and availability of the systems and services which process and store the personal data
- Privacy by design includes minimisation of data sources, raw data, data storage and processing of only the necessary data

- The proper execution of a Privacy Impact Assessment (PIA) should be supported by a risk management system which identifies and reduces the privacy risks
- Organisations should use measures such as pseudonymisation and encryption to protect the privacy of their data
- Implement a real-time detection and response system to protect against cyberattacks and unauthorised access

2.8.2 Standards

Adoption of the following standards can help an organisation to achieve regulatory compliance from a security and privacy perspective:

IEEE 802.15.6

IEEE 802.15.6 is the first published standard for short-range wireless-based medical and non-medical applications. This standard aims to provide better quality of service with strong security for sensitive health information by assuring authentication, integrity and confidentiality for WBAN based applications. This standard also defines new physical and MAC layers for WBAN applications which will help to standardise the frequency range selection process for communication for different countries. The standard also provides three levels of security properties. Level 0 is named *"unsecured communication*", the lowest security level where data is transmitted without authentication and encryption. Level 1 is named *"authentication only"* where data is transmitted with authentication only and has no encryption. Finally, level 2 is called *"authentication and encryption"* where data is transmitted securely with authentication and encryption. This standard does not provide any guidelines to assure the privacy of the data. Additionally, this standard does not provide guidelines to achieve regulatory requirements while developing a WBAN based healthcare application.

IEC 62304

IEC 62304 provides guidelines for each stage of the medical device software lifecycle with activities and tasks required for the safe design and maintenance of medical device software (IEC 62304, 2019). This standard is recognised by the FDA, EU and other regulatory agencies across the world. IEC 62304 recommends that organisations establish and maintain a risk management process to manage risk associated with security. The process should provide a methodology to identify the vulnerabilities, evaluate the associated threats, and implement risk controls to mitigate these threats. Finally, the process should also monitor the effectiveness of the risk control.

NIST 800-53

The NIST 800-53 standard provides security and privacy controls to protect applications, data, assets and organisations from a diverse set of attacks, threats and risks (NIST SP800-53, 2020). These controls support the development of secure and resilient federal information systems that meet the requirements set by the Federal Information Security Management Act (FISMA). This guideline applies to any component of a system which stores, processes and transmits information. NIST SP 800-53 provides controls for the operational level, the technical level and the management level of information systems. These controls are used to assure confidentiality, integrity and availability of the federal information system. This guideline adopted a multi-tiered risk management approach and designed the controls to align with SP 800-37 - a risk management framework of information system and organisation for security and privacy. By adopting a risk management approach, each control is classified into three different classes: Low, Medium or High based on their impact. SP 800-53 also introduces the concept of a security baseline which will help to create the security controls baseline depending on operational need, functional need and the most common types of threats facing an information system.

ISO 27002

ISO 27002 is an information security standard developed by the International Organization for Standardization (ISO) which provides best practice recommendations and information security controls to assure confidentiality, integrity, and availability of data (ISO/IEC 27002, 2017). This standard is designed for organisations to use as a reference to guide organisations to select, implement, and manage controls based on ISO/IEC 27001 to minimise security risk. Additionally, this standard also helps to develop industry and organisation-specific information security management guidelines by considering their specific information security risk environment.

FDA premarket and postmarket guidelines

The FDA provides premarket and postmarket guidelines for organisations and developers that need to be considered during the development lifecycle of a medical device or healthcare application. The premarket guidance (FDA, 2018) outlines the following key security and privacy related recommendations for medical device manufacturers:

- To employ a risk-based approach to the design and development of medical devices with appropriate cybersecurity protections.
- Take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the product’s lifecycle.
- Identify the assets, threats, and vulnerabilities.
- Perform an impact assessment of the threats and vulnerabilities on device functionality and end-users.
- Assess the likelihood of a threat and of a vulnerability being exploited.
- Determine the risk levels and suitable mitigation strategies.

As cybersecurity risks to medical devices are continuously evolving, it is impossible to mitigate the risk within the premarket controls alone. Therefore, the FDA provides the following key guidance for manufacturers as part of postmarket medical device development (FDA, 2016):

- Take an approach to monitor the cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk.
- Identify and assess the threats and vulnerabilities being exploited.
- Take a holistic approach to detect and assess the threat sources.
- Establish a communication process for incident response.
- Design a verification and validation process for software updates and patches used to remediate the vulnerabilities.

IEC 80001-1:2010

IEC 80001-1 *Application of risk management for IT-networks incorporating medical devices* was introduced in 2010 to address risks associated with medical devices when connecting to IT-networks (IEC 80001-1, 2015). The framework aims to help organisations define the risk management roles, responsibilities, and activities to achieve medical device safety and security. IEC/TR 80001-2-2 (IEC 80001-2-2, 2011) is a technical report that provides background processes to address security risk related capabilities for connecting medical devices to IT-networks. IEC 80001-1:2010 was primarily developed for applications which operate within a healthcare delivery organisation’s IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media.

IEC/TR 80001-2-8

IEC/TR 80001-2-8 is a technical report which provides guidance to Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) to establish security controls for applications with security capabilities which are outlined in IEC/TR 80001-2-2 (ISO/IEC 80001-2-8, 2016). A security control is a safeguard or countermeasure designed to protect security and privacy of an information system. Security capabilities are a combination of security controls implemented by technical (functionality in hardware, software, and firmware), physical (physical devices and protective measures), and procedural (procedures performed by individuals) means. IEC/TR 80001-2-2 is a technical report that provides background processes to address security and risk related capabilities for connecting medical devices to IT-networks (IEC 80001-2-2, 2011). The IEC/TR 80001-2-2 technical report presents a total of nineteen high-level security capabilities to maintain the confidentiality, integrity and availability of data. It also provides roles and responsibilities of HDOs, MDMs and IT-Network vendors in risk management:

a) HDOs with a catalogue of management, operational and administrative security controls to maintain the effectiveness of a security capability for a medical device on a medical device IT-network

b) MDMs with a catalogue of technical security controls for the establishment of each of the 19 security capabilities

The IEC/TR 80001-2-8 technical report was developed to establish security controls for the 19 security capabilities mentioned in the IEC/TR 80001-2-2. These controls come from six different international standards. The IEC/TR 80001-2-8 report uses the following international standards to develop the security controls:

1) NIST SP 800-54 revision 4
2) ISO/IEC 15408-2:2008
3) ISO/IEC 15408-3:2008
4) ISO/IEC 27002:2013
5) ISO 27799:2008
6) IEC 62443-3-3:2013

The intent of these security controls is to protect confidentiality, integrity and availability of the data and information system. All nineteen security capabilities might not be required in every application. Security capabilities and security controls should be selected based on a risk assessment. The IEC/TR 80001-2-8 technical report does not provide adequate details for implementing these risk controls. Therefore, this technical report refers to other standards for the implementation details of the risk control. For example, the ISO/IEC 80001-2-8 proposes the use of a key management process as a risk control to generate, distribute and revoke a cryptographic key. To achieve this the standard refers to section 10.1.2 of ISO 27002 for further details. Section 10.1.2 of ISO 27002 provides very high level and generic details about a key management process and does not provide any information about how the key will be generated and how the key will be transferred from the mobile application to the sensor device. ISO 27002 again refers to another standard ISO/IEC 11770 for further details about key management, however ISO/IEC 11770 only outlines the details about the key generation and not about the key transfer. From the above example, the developer needs to review three different standards to find implementation details for key management.

ISO 14971

ISO/IEC 14971 *Medical devices - Application of risk management to medical devices* (ISO 14971, 2018) provides guidance to medical device manufacturers to establish a risk management process to identify and mitigate the safety risk. The standards recommend performing the following activities to manage safety risks within the medical device:

- The risk management plan
- Risk identification
- Risk estimation
- Risk evaluation
- Risk control

- Risks arising from risk control measures
- Verification of effectiveness of risk control measures
- Residual risk evaluation
- Risk/benefit evaluation

The only drawback concerning this study is that ISO 14971 only focuses on safety-related risk; this standard does not provide any guidance to manage security and privacy related risk within the medical device. The process presented in the standard can be helpful to develop a new risk management framework to assure security and privacy.

AAMI TIR57

AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices (AAMI TIR57, 2016). AAMI TIR57 was developed with guidelines provided by ISO 14971 (ISO 14971, 2018) and NIST SP 800-30 Revision 1(NIST:800-30, 2012) - *security risk management process developed for traditional IT systems.* The goal of AAMI TIR57 is to assist manufacturers with the following key outcomes:

1) Identification of assets, threats and vulnerabilities
2) Estimation and evaluation of associated security risk
3) Selection of security risk controls
4) Monitoring the effectiveness of the security risk controls

2.8.3 Summary

The 800 series under Title 21 of the CFR outlines the regulations which govern medical devices within the US and are enforced by the FDA. The FDA recognises that the security and privacy of medical devices is a shared responsibility among stakeholders, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices. Medical devices should be designed to protect assets and functionality, and to reduce the risk of loss of authenticity, availability, integrity and confidentiality. Additionally, the US Department of Health and Human Services introduced the HIPAA act to enforce regulations for governing electronically managed patient information in the healthcare industry, and includes privacy and security protection of PHR data. Title II of HIPAA provides five rules to prevent fraud and abuse within the healthcare system. Furthermore, the EU MDR assures high standards of safety, security, and quality of medical devices being marketed within the EU for human use. The EU MDR states that medical device software should be developed in accordance with the state-of-the-art principles of the development life cycle, risk management, including information security, verification and validation. The EU MDR also states that manufacturers need to implement proper safeguards to avoid unauthorised access, disclosure, dissemination, alteration or loss of information and personal data processed. Additionally, the EU introduced the GDPR in May 2018. The purpose of the GDPR is to assure data protection and privacy for EU citizens.

Section 2.8.2 presents a list of standards which can help an organisation achieve regulatory compliance from a security and privacy perspective. IEEE 802.15.6 is the first published standard for WBAN based medical and non-medical applications. While the IEEE 802.15.6 aims to provide a better quality of service with strong security for sensitive health information by assuring authentication, integrity and confidentiality for WBAN based applications, it does not provide any guidelines to assure the privacy of the data and achieve regulatory requirements while developing a WBAN based healthcare application. NIST SP 800-30 is a widely used risk management framework to manage and provide guidance to manage security risk within both the application and organisation. While NIST SP 800-30 provide controls to protect applications, data, assets and organisations from a diverse set of attacks, threats and risks, it does not outline any guidelines which are tailored for healthcare organisations to manage security and privacy risk in healthcare applications. ISO 14971 guides medical device manufacturers to establish a risk management process to identify and mitigate safety risks. The only drawback concerning this study is that ISO 14971 only focuses on safety-related risk; this standard does not provide any guidance to manage security and privacy related risk within the medical device. IEC 80001-1 provides guidance on managing risks associated with medical devices within a healthcare delivery organisation's IT network, whereas WBAN applications may operate in public, open networks using short-range communication media. AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices. A WBAN application consists of resource-constrained sensor devices with limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications. This framework does not provide any guidance for managing security and privacy risks for resource-constrained sensor devices.

2.9 Challenges For Adopting a Security and Privacy Framework

Adopting a cybersecurity framework helps organisations to create a baseline for measuring the effectiveness of security and privacy controls as well as to meet compliance requirements. Adopting a cybersecurity framework requires overcoming a range of both technical and organisational barriers (Townsend, 2017). According to Townsend (2017), 95% of organisations have faced issues in implementing the chosen cybersecurity framework due to lack of trained staff, lack of budget and lack of management support. In MacMahon et al., (2018), the authors conducted three case studies within Healthcare Delivery Organisations (HDO) who attempted to implement the IEC 80001-1 risk management framework for IT-networks incorporating medical devices. The case studies were carried out in HDOs of varying sizes and in different geographical locations to identify the barriers to adopt the IEC 80001-1 risk management framework. These barriers include:

- A lack of motivation and support from management teams due to a perceived lack of return on investment
- Existing standards are too complicated and complex to implement, and lack implementation detail
- Existing standards are too abstract and not tailored to the organisation's needs

Chen and Benusa (2017) state that small organisations have limited knowledge about information security and privacy frameworks, and they often failed to perform risk assessments or to create security and privacy policies. The authors also state that small organisations are facing major challenges complying with regulations. The authors suggested that the management team of a small organisation should take regulatory compliance seriously and be self-educated on the relevant regulations and standards. The authors also suggested seeking professional advice when confusion or different interpretations of a clause occur. Table 2-7 presents the list of challenges identified from the literature review.

Table 2-7: Challenges for adopting security and privacy framework (Literature review)

Challenges	Sources
Lack of trained staff, responsibilities, budget, and management support	(Townsend, 2017), (Holden, 2014), MacMahon et al., (2018), (Q. Chen et al., 2016) (Shah and Khan, 2020), (Eom and Lee, 2017) (Benz and Chatterjee, 2020), (Chen and Benusa, 2017) (Mariani and Mohammed, 2015), Ključnikov et al., (2019)
The existing standards are too complex and complicated to implement	MacMahon et al., (2018), (Eom and Lee, 2017) (Aljohani and Blustein, 2018), (Skierka, 2018) (Thapa and Camtepe, 2021)
Limited knowledge about market-specific regulatory requirements, security standards, and policies	(Chen and Benusa, 2017), (Skierka, 2018) (Supriya and Padaki, 2016), Stevovic et al., (2013) Abraham et al., (2019)
Standards outline each security control at a very high-level with limited amount of implementation details	MacMahon et al., (2018), (Mariani and Mohammed, 2015)
Identification of appropriate security controls with respective implementation details to assure CIA and privacy of data	Aceto et al., (2018)
Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage	(Thapa and Camtepe, 2021) (Supriya and Padaki, 2016) Iyengar et al., (2018) Paquette et al., (2011)

In Mariani and Mohammed (2015), the authors conducted a case study to investigate security breaches that occurred in various US based healthcare organisations. The investigation showed that each of the breaches were caused by equipment containing unencrypted data being lost or stolen, or systems with inadequate protections being exploited by hackers. The authors concluded that the implementation of an effective information security program and system security controls continued to pose a significant challenge due to the lack of motivation from the leadership and development team. Furthermore, the authors also identified that encryption was not implemented due to a lack of adequate implementation details and a lack of knowledge and motivation from the leadership and development team.

2.10 Security and Privacy Risk Management Framework Properties

The National Institute of Standards and Technology (NIST) defines a cybersecurity framework as voluntary guidance designed for an organisation based on existing standards, guidelines, and practices to manage and reduce cybersecurity risks. According to NIST a cybersecurity framework should be customisable based on the organisation’s risks, situation and needs (NIST CSF, 2021). As organisations will have unique risks, threats, vulnerabilities, and risk tolerance, implementing a framework and its outcomes will vary from organisation to organisation. In Garrabrants *et al.* (1990) and (Lichtenstein, 1996), the authors present seven properties of a risk management framework which are presented below:

- Consistency: Given a particular system configuration, results obtained from the independent analysis will not significantly differ.
- Usability: The framework should be understandable, easy to use, simple and capable of handling errors. It should be usable and understandable by the available resources.
- Adaptability: The framework must be able to adapt to an organisation’s needs.
- Feasibility: The framework should be feasible in terms of its availability, practicality and scope. The required data is available and can be economically gathered.
- Completeness: The framework should consider all relevant aspects and elements of a system’s information security.

- Validity: The framework should produce valid results, with recommendations for safeguards. Validity is composed of relevance, scope and practicality.
- Credibility: The framework results must be acceptable to security personnel in the organisations and the management. They must believe that the framework is producing credible and reliable results.

NIST SP 800-30 is a widely used risk management framework to manage and provide guidance for conducting risk assessments of federal information systems and organisations. The goal of this framework is to provide a foundation for assessing and mitigating risks identified within IT systems, which will help organisations better manage IT-related risks (NIST:800-30, 2012). NIST SP 800-30 consists of framing the risks, assessing risks, responding to risks, and monitoring the risks. Among them, the framing risks stage is used to produce a risk management strategy to assess the risks. The second component is to assess the risk, which includes identifying the threats, internal and external vulnerabilities, the impact, or harm that may occur if the threat exploits the vulnerabilities and the likelihood of the risk. The third component is defining a mitigation strategy to respond to the risk identified from the second component. Finally, the fourth component is to determine a strategy to monitor the risk over time and measure the ongoing effectiveness of the risk-mitigation strategy.

ISO 27005 Information technology — Security techniques — Information security risk management is developed by the International Organization for Standardization (ISO) to manage risks that can compromise the organisation's information security (ISO 27005, 2015). ISO 27005 consists of five key phases: risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring. The risk assessment phase includes:

- Identification of the risk management context (organisational boundaries, systems, etc.)
- Identification of assets
- Identification of threats and vulnerabilities

- Identification of risk likelihood
- The evaluation and estimation of potential risks

In the risk treatment phase, the organisation implements the risk treatment plan, which includes implementing selected controls to reduce the risk to an acceptable level.

OCTAVE is a risk assessment methodology to identify, manage and evaluate information security (Alberts *et al.*, 2003). OCTAVE is an asset-driven evaluation approach; using this approach, an organisation can make information-protection decisions based on the risks to the confidentiality, integrity, and availability of critical information-related assets. The OCTAVE approach is driven by two aspects: operational risk and security practices. The OCTAVE approach consists of the following steps:

- Identify information-related assets
- Focus risk analysis activities on those assets judged to be most critical to the organisation
- Consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organisational and technological) that can expose assets to threats
- Evaluate risks in an operational context - how they are used to conduct an organisation's business and how those assets are at risk due to security threats
- Create a practice-based protection strategy for organisational improvement as well as risk mitigation plans to reduce the risk to the organisation's critical assets

Table 2-8: Comparison of the risk management framework phases

Risk management framework	Risk assessment approach	Phases
NIST 800-30	Qualitative or Quantitative	System Characterisation Threat Identification Vulnerability Identification Control Analysis Likelihood Determination Impact Analysis Risk Determination Control Recommendations Results Documentation
ISO 27005	Qualitative or Quantitative	Risk assessment Risk treatment

Risk management framework	Risk assessment approach	Phases
		Risk acceptance Risk communication Risk monitoring
OCTAVE	Qualitative	Build Asset-Based Threat Profiles Identify Infrastructure Vulnerabilities Develop Security Strategy and Plans
AAMI TIR 57	Qualitative or Quantitative	Identification of assets, threats and vulnerabilities Estimation and evaluation of associated security risk Selection of security risk controls Monitoring the effectiveness of the security risk controls

Table 2-8 indicates that risk management frameworks are using either a qualitative or a quantitative approach for conducting risk assessment. A qualitative assessment approach uses subjective values with a scale of qualifying attributes (e.g. Very Low, Low, Medium, High, Very High) to describe the impact and likelihood of potential consequences of threats and vulnerabilities. The value of the impact and likelihood depends on the experience, expertise and competence of the person conducting the risk assessment. The qualitative assessment approach is very easy and less time consuming to perform compared to quantitative, as this approach does not require any special tools or methods. Quantitative risk assessments use a scale with numerical values based on a set of mathematical methods, rules and historical incident data. This approach is usually expressed in a monetary term which reflects the amount of money an organisation may lose over a time period if the threat event occurs, or a vulnerability is exploited. The quality of the analysis depends on the accuracy of the numerical values, historical incident data and the validity of the methods used. The comparison in Table 2-8 also showed that there are only minor differences between the existing risk management frameworks. In the first phase, each framework requires an inventory of relevant infrastructure elements and definition of the organisation’s mission and goal. From a high-level perspective, the subsequent phase requires the identification of the threats and respective vulnerabilities. The identified threats and vulnerabilities will then be used to determine the risk's impact level and respective control for mitigating the risk. In the final phase, the organisation will define the strategy to monitor the effectiveness of the risk controls.

2.11 Research Questions Revisited

This chapter partially provides answers to Research Sub-Questions 1, 2, and 3.

RSQ 1*: What challenges are faced by developers of wireless body area network applications to assure the security and privacy of PHR data?*

The literature review indicates that developers face the following challenges to assure security and privacy of a WBAN application:

- WBAN applications can be affected by a total of eleven types of attack. Among them, denial-of-service, eavesdropping, replay attacks, and data modification attacks are as the most common attacks on WBAN applications
- There are twenty-two requirements that need to be considered for assuring the security and privacy of WBAN applications
- Developers also face challenges to implement safeguards for mitigating the threats and vulnerabilities due to having limited knowledge about security and privacy standards
- Existing standards consist of a vast number of controls, and these standards are very complex and complicated to implement
- Developers face challenges to identify the appropriate security and privacy controls to mitigate the threats and vulnerabilities
- Existing standards outline each security control at a very high-level with limited amount of implementation details
- Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage

RSQ 2: *What frameworks, methods and techniques are used to assure data security and privacy for wireless body area networks?*

The literature review identified a total of six risk management frameworks: ISO/IEC 80001-1:2010, AAMI TIR57, ISO 14971, ISO 27005, OCTAVE and NIST 800-30. An initial analysis found that only two of these six frameworks were 'healthcare specific' security and privacy risk management frameworks: ISO/IEC 80001-1:2010 and AAMI TIR57. Among them, IEC 80001-1 guides managing risks associated with medical devices when connecting to IT networks. The framework aims to help organisations define the risk management roles, responsibilities, and activities to achieve medical device safety and security. IEC 80001-1:2010 was primarily developed for applications within a healthcare delivery organisation's IT network, whereas WBAN applications may operate in public, open networks using short-range communication media. IEC 80001-1:2010 does not provide any guidelines for assuring security and privacy in resource-constrained sensor devices that communicate over Bluetooth.

AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices. AAMI TIR57 was developed with guidelines provided by ISO 14971 and NIST SP 800-30. This framework does not provide any guidance for managing security and privacy risks for resource-constrained sensor devices. A WBAN application consists of resource-constrained sensor devices with limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications.

ISO 14971 guides medical device manufacturers to establish a risk management process to identify and mitigate safety risks. The only drawback concerning this study is that ISO 14971 only focus on safety-related risk; this standard does not provide any guidance to manage security and privacy related risk within the medical device.

NIST SP 800-30 is a widely used risk management framework to manage and provide guidance for conducting risk assessments of information systems and organisations. This framework aims to provide a foundation for assessing and mitigating risks identified within IT systems, which will help organisations to better manage IT-related risks. NIST SP 800-30 provides generic guidelines to manage security risk within both the application and organisation. These guidelines can be used to develop a new risk management framework and have been adopted by ISO 14971 and AAMI TIR7. A limitation of NIST SP 800-30 is that it only provides guidelines to manage information systems and organisations' security and does not outline any guidelines for managing privacy related risk in healthcare applications.

ISO 27005 was developed to manage risks that can compromise the organisation's information security. ISO 27005 consists of five key phases: risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring to manage the security risk. This risk management framework aims only to manage the organisation’s information security. This framework does not provide any guidelines to manage security and privacy related risks within an application.

OCTAVE is a risk assessment methodology for identifying, managing and evaluating information security. OCTAVE is an asset-driven evaluation approach; using this approach, an organisation can make information-protection decisions based on the risks to the confidentiality, integrity, and availability of critical information-related assets. But, OCTAVE does not have any guidelines to manage security and privacy risks for medical devices.

RSQ 3: *What should a WBANSecRM framework contain to assist wireless body area network application developers in assuring security and privacy and put them on the path to regulatory compliance?*

‘Title 21 CFR part 820 - Quality System Regulation’ states that the medical device manufacturer needs to employ a cybersecurity risk management program to reduce the risk of losing authenticity, availability, integrity and confidentiality. The literature review indicates that a framework should be easy to understand, easy to use, and easily adaptable by organisations. The framework also needs to produce valid and credible results for the organisations that the security personnel will accept. The risk management framework should use a qualitative and/or quantitative approach for conducting risk assessment. Furthermore, the framework should also consist of the following phases to assure security and privacy:

- Identification of assets
- Identification of threats and vulnerabilities
- Estimation and evaluation of associated security risk
- Risk treatment
- Risk acceptance
- Selection of security and privacy risk controls
- Develop the implementation details for security and privacy risk controls
- Implement the selected security and privacy risk controls
- Monitoring the effectiveness of the security risk controls

2.12 Summary

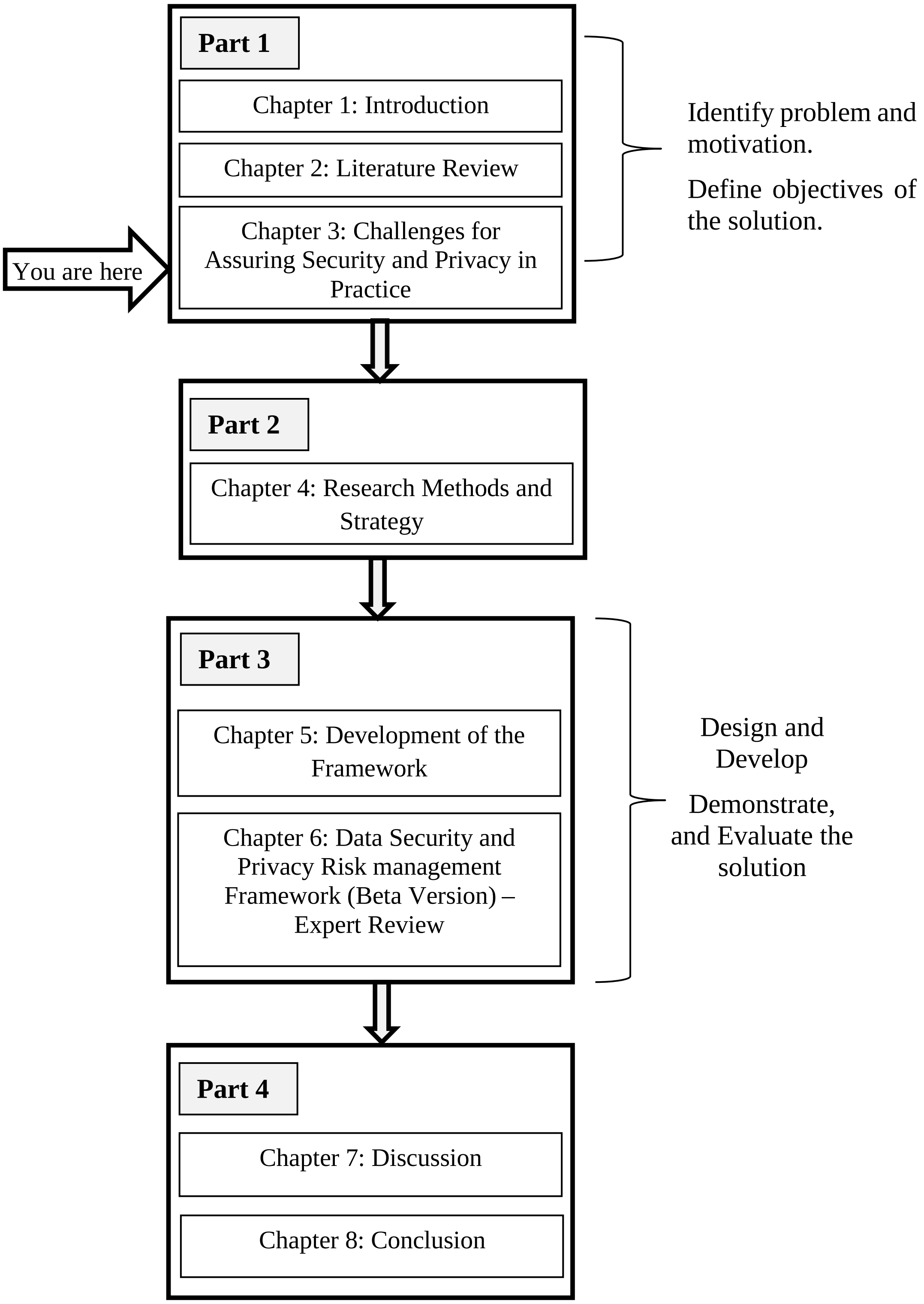
This chapter begins by outlining the approach employed to conduct this literature review. This approach is a lightweight version of a systematic literature review developed by Barbara Kitchenham.

The literature review indicates that the most challenging issues related to developing a WBAN based healthcare application are energy efficiency, antenna design, assuring the quality of service, and security and privacy. Managing the security and privacy of patient health records is a major concern for regulators and developers. In addition, medical device manufacturers, healthcare organisations and application developers need to implement proper safeguards to reduce the risks in the event of a cyber-attack. The literature review indicates that a WBAN application can be affected by a total of eleven types of attack. Denial-of-service, eavesdropping, replay attacks, and data modification attacks are as the most common attacks for WBAN applications. The literature review also indicates that there are twenty-two types of requirements to assure the security and privacy of WBAN applications. The most referenced security and privacy requirements are data confidentially, data integrity, data availability, authentication, encryption, data privacy, key management and access control. The least addressed security and privacy requirements are a firewall, physical protection, auditing, client platform security, and anonymity.

The literature review also indicates that none of the existing solution approaches addresses all the security and privacy requirements. Various standards and guidelines propose lists of security and privacy controls for implementing proper safeguards of PHR data. Due to the vast lists of security and privacy controls with lack of implementation details, implementation of these controls is complex and challenging. The literature review also indicates that existing risk management frameworks for healthcare applications were primarily developed for applications which operate within a healthcare delivery organisation's IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media. When a WBAN application operates in an environment where many people have open internet access, this leaves them vulnerable and open to many types of attacks and threats. Additionally, open connectivity creates a large attack surface. WBAN applications consist of resource constrained sensor devices which have limited memory and computational power and the literature review indicates that none of the frameworks provide guidance for managing security and privacy risks for resource-constrained sensor devices.

Finally, this chapter provides a review of existing risk management frameworks to identify the properties a risk management framework should contain. The literature review indicates that each framework requires an inventory of relevant infrastructure elements and definition of the organisation's mission and goal. From a high-level perspective, the subsequent phase requires the identification of the threats and respective vulnerabilities. The identified threats and vulnerabilities are then used to determine the risk's impact level and respective control for mitigating the risk. In the final phase, the organisation will define the strategy to monitor the effectiveness of the risk controls.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
You are here
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

3 Challenges for Assuring Security and Privacy in Practice

3.1 Introduction

The literature review indicates that adopting a cybersecurity framework is a challenging task due to the various technical and organisational barriers that need to be overcome. It requires a thorough understanding of the organisation's specific needs and environment, as well as the technical aspects of implementing and maintaining a cybersecurity framework. Additionally, organisational barriers such as resistance to change, lack of resources, and insufficient communication can hinder the adoption process. Therefore, it was decided to investigate one WBAN based healthcare application development organisation. The investigation aimed to gain insights into the challenges faced by the WBAN application development organisation in implementing safeguards to ensure security and privacy. By understanding these challenges, the investigation can provide partial answers to RSQ1: *"What challenges are faced by developers of wireless body area network applications in assuring the security and privacy of PHR data?"*.

In the section 3.2, the choice of interview selected for this part of the research and the sample size are discussed. Additionally, the next section also outlines the organisation selected for the interview along with the steps to develop the questionnaire. On return of the completed questionnaire, the comments received from the interviewee was analysed by the author of this study. The methodology for conducting this analysis is presented in section 3.3. Finally, section 3.4 outlines the challenges identified for assuring security and privacy for a WBAN application.

3.2 Data Collection

To understand the challenges faced by the organisation in implementing safeguards to assure security and privacy of a WBAN application, it is necessary to collect data from the WBAN application development organisation. The main data collection methods are conducting interviews, observing participant behavior, and reviewing documents. Among them, interviews are the widely used qualitative method for data collection (Braun and Clarke, 2013 pp.77).

3.2.1 Qualitative Interviews defined

Qualitative interviews are a research method that enables researchers to gather detailed insights into an individual's experiences, perspectives, and behaviours. These interviews involve engaging participants in structured, semi-structured, or unstructured conversations, allowing for a more in-depth understanding of the topic being studied (Rubin and Rubin, 2012 pp3). To ensure a diverse and informative range of perspectives on a research topic, researchers often use purposeful sampling to select participants. Moreover, when conducting qualitative interviews, ethical considerations such as informed consent and participant anonymity are crucial aspects to be taken into consideration. Qualitative interviews are an essential tool for researchers to uncover underlying motivations, cultural nuances, and social contexts that quantitative methods may not capture fully. They play a crucial role in theory-building, hypothesis generation, and developing a holistic understanding of complex phenomena (Creswell and Creswell, 2018).

3.2.2 Interview Structure and Question Types

There are various ways in which interviews can be structured, including structured, semi-structured, and unstructured. Additionally, interviews can be conducted using closed or open-ended questions. However, before diving into the interview structure and question types used, this section provides a closer look at these interview structures and question types.

3.2.2.1 Interview Structure

Structured Interviews: In structured interviews, the researcher follows a fixed, standardized set of questions with little deviation. This method is similar to a survey that includes closed-ended questions. Structured interviews are commonly utilised when the researcher requires consistent responses or quantitative data from the participants (Braun and Clarke, 2013 pp78).

Semi-structured Interviews: Semi-structured interviews are popular among qualitative researchers, as they offer a balance between a pre-defined framework and the freedom to capture participants' experiences and perspectives in detail (Braun and Clarke, 2013 pp78). Such interviews involve using a set of key questions or topics as a guide while allowing the interviewer to ask follow-up questions and modify the conversation based on the participant's responses. This method provides a consistent approach while enabling in-depth exploration (Rubin and Rubin, 2012 pp149).

Unstructured Interviews: Unstructured interviews offer high flexibility, as there are no pre-set questions for the researcher to follow. Instead, the conversation flows freely, with the researcher having only a broad topic in mind. This allows for open exploration of the participant's perspective and encourages them to share their thoughts, feelings, and experiences about the topic at hand. Such interviews aim to collect narrative data, and the researcher engages in open-ended conversations with participants to achieve this goal (Braun and Clarke, 2013 pp78).

3.2.2.2 Interview Question Types

Closed Question: Closed questions are designed to elicit a precise, concise answer, often in the form of a "yes" or "no" response or a short piece of information. They are particularly useful in situations where the researcher needs to gather specific information quickly and efficiently. Closed questions can help to establish clear, objective data points and can be useful in quantitative research (Braun and Clarke, 2013 pp84).

Open Question: Open questions are designed to allow respondents to provide answers in their own words and are not limited to specific options or answers (Creswell and Creswell, 2018). They encourage a more detailed and open-ended response and enable the respondent to express their thoughts, feelings, or opinions in greater depth. Open questions are often used in qualitative research to gather detailed information, explore ideas, and elicit subjective perspectives.

3.2.3 Organisation Profile

Company A is a startup company that has quickly grown to be one of the leading suppliers of performance tracking and monitoring systems for elite sports. Due to the success of their systems, they are expanding into the area of cloud based WBAN application. The system will enable multiple users with access to a mobile application or a computer desktop web-browser to monitor the performance, movement and health information of elite sports players in real time through the cloud system. This will also allow for seamless monitoring of various biometric parameters and will aid in the quick diagnosis and treatment of any medical conditions. As part of the interview process, a group of three individuals from Company A participated in the session to help achieve the objectives. The group was comprised of the CTO, Tech Lead, and Senior Developer.

The CTO is a highly experienced professional with over 25 years of expertise in product development. Throughout his career, he has demonstrated exceptional leadership skills, having led product development teams for 19 years. He is a strategic thinker, with a strong focus on creativity and innovation, which has led to the successful implementation of many novel solutions. He has led multi-disciplinary engineering teams, including hardware, FPGA, software, mechanical, and manufacturing, and his expertise in these fields has been instrumental in delivering high-quality products.

The technical lead has over 12 years of experience in product development. He is an expert in making critical architectural and design decisions. He supervises system modifications and ensures that all changes are implemented efficiently and effectively, guaranteeing that the system runs smoothly. In addition to his technical responsibilities, the technical lead is also involved in conducting regular security and privacy audits. These audits help to identify any potential security and privacy issues, ensuring that the application's security and privacy features are up-to-date and robust. By ensuring that the application meets the highest security and privacy standards, the technical lead plays a crucial role in maintaining the application's integrity and protecting user data.

The senior developer is an outstanding software engineer who is highly competent and motivated to develop software. His expertise includes developing new software and improving the existing systems. He has over eight years of experience in the software development industry, working on a wide range of web, mobile, and desktop applications. He involved in all aspects of the development process, from planning and requirements gathering to writing and testing code.

3.2.4 Creating Interview Guide

The strategy used to develop the questions is based on the strategy identified by Catherine Dawson (2002, p.69). The question development phase contained eight steps illustrated in Figure 3-1. The first step involved considering the purpose of the interview and what information the researcher sought from the interview. The purpose of the interview is to identify the challenges faced by the organisation to assure security and privacy when developing WBANs.

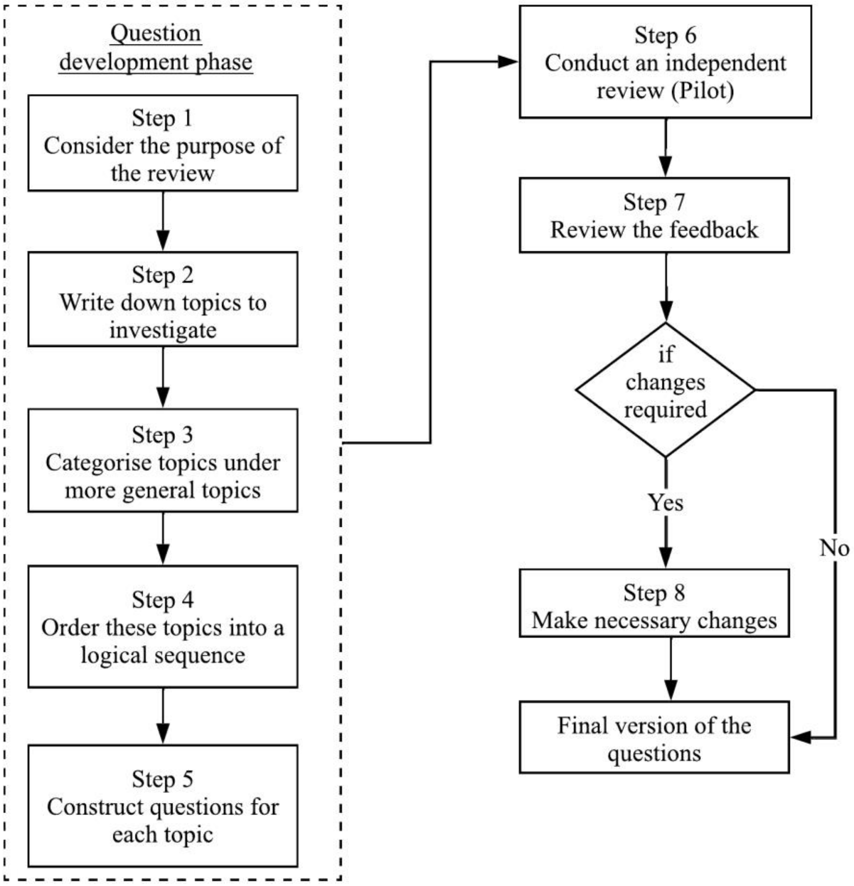

Question development phase
Step 1
Consider the purpose of the review
Step 2
Write down topics to investigate
Step 3
Categorise topics under more general topics
Step 4
Order these topics into a logical sequence
Step 5
Construct questions for each topic
Step 6
Conduct an independent review (Pilot)
Step 7
Review the feedback
if changes required
Yes
No
Step 8
Make necessary changes
Final version of the questions

Figure 3-1: Interview questionnaire development method

Step 2 of this phase was to identify the topics to be investigated during the interview. Below is the list of topics that were identified:

- Security and privacy requirements in software development process
- Healthcare legislation, such as HIPPA and GDPR
- Knowledge about security and privacy standards
- Knowledge about developing system architecture of the application
- Understanding of the data flow and respective assets for the application
- Identifying the security and privacy controls
- Prioritise the security and privacy controls
- Implementing security and privacy controls on resource constrained devices

Step 3 involved taking the topics generated in Step 2 and categorising them under more general topics (henceforth known as categories) as depicted in Table 3-1. This was achieved by merging strongly linked topics. Methodological challenges relate to the difficulties companies found in integrating security identification, analysis, testing and monitoring in their development methodology. Organisational challenges relate to company's policies, factors about market and external stakeholders. Technical challenges relate to specific security concerns when designing and implementing WBAN applications.

Table 3-1: Topics redefined to categories for developing the questionnaire

Category No.	**Category**	**Step 2 Topic**
1	Methodological	1,6,7
2	Organisational	2,3
3	Technical	4,5,8

Step 4 of the question development phase is to order the categories into a logical sequence, generally moving from the more general to the specific. The resulting sequence from this step is presented in Table 3-1 above.

Step 5 of the question development phase involved constructing questions around each category. The questions are constructed with a combination of open-ended and closed-ended questions. In general, the questions contained a greater proportion of open-ended questions and were kept short, neutral and to the point. With the combination of closed and open-ended questions, this step produced seven questions listed in Appendix G.

Step 6 of the questionnaire development was to have the questionnaire independently reviewed. This review was completed by a member of RSRC. The reviewer had extensive experience and expertise in software processes for healthcare applications and developing interview questionnaires. A copy of the questionnaire and a statement outlining the purpose of the review was provided to the reviewer to determine how well the questionnaire fulfilled its purpose and assure that it did not contain ambiguity. In step 7, the reviewer commented that no changes were required after reviewing the questionnaire. The final seven questions are presented in Appendix G.

3.3 Data Analysis

The interview response was received in electronic format via email, where review comments were the result of answers to a combination of closed and open-ended questions. Due to the nature of the responses, the answers to the open-ended questions consisted of text with similar concepts in different text locations. The challenges were then to structure the comments into meaningful and analysable data from which conclusions could be drawn. The five-stage approach used to analyse the interview response is detailed in Figure 3-2. This was developed based on the guidelines presented by Saunders, Lewis and Thornhill, (2009, pp.478) for analysing qualitative data.

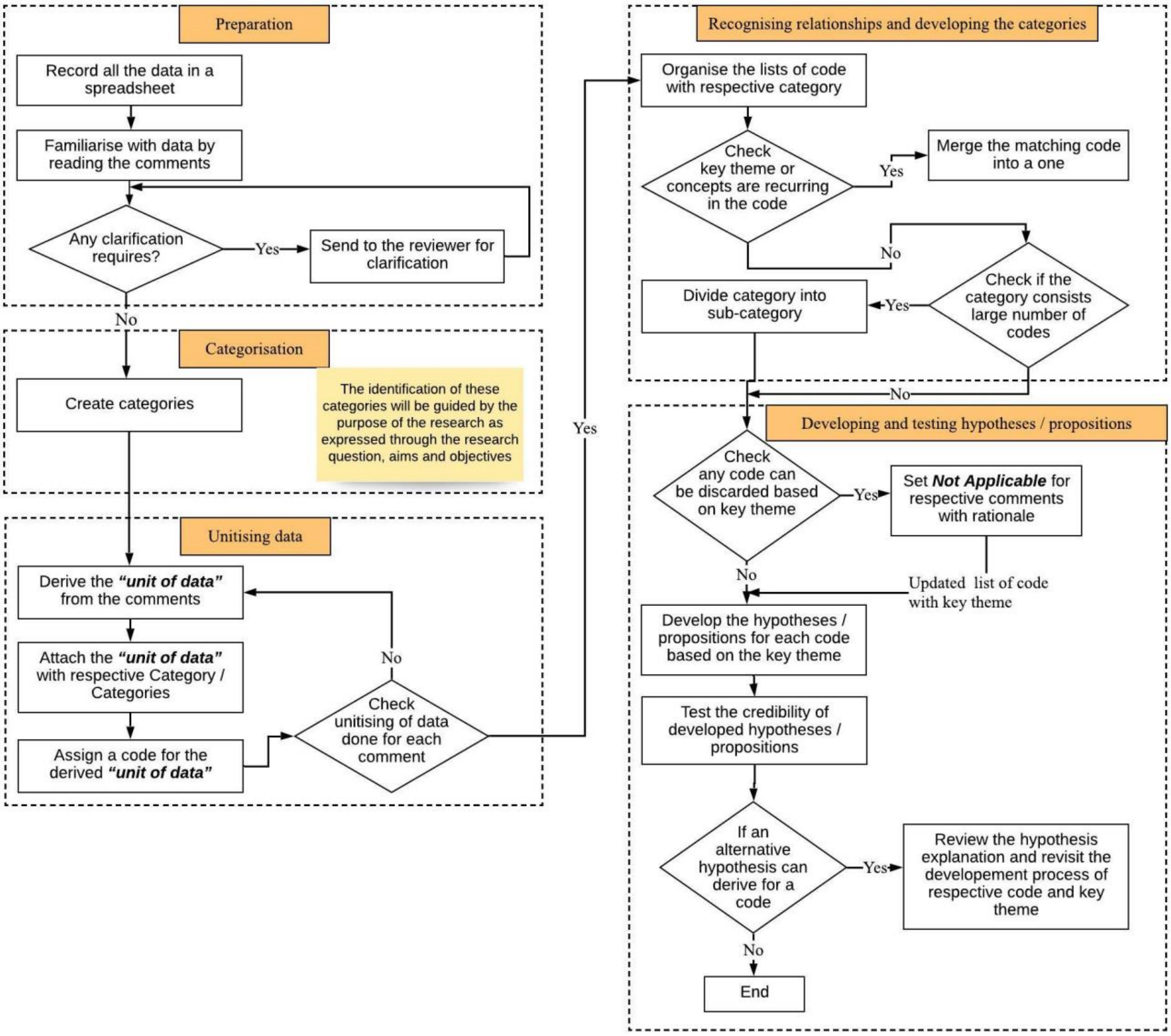

Preparation
Record all the data in a spreadsheet
Familiarise with data by reading the comments
Any clarification requires?
Yes
Send to the reviewer for clarification
No
Categorisation
Create categories
The identification of these categories will be guided by the purpose of the research as expressed through the research question, aims and objectives
Unitising data
Derive the "unit of data" from the comments
Attach the "unit of data" with respective Category / Categories
Assign a code for the derived "unit of data"
Check unitising of data done for each comment
No
Yes
Recognising relationships and developing the categories
Organise the lists of code with respective category
Check key theme or concepts are recurring in the code
Yes
Merge the matching code into a one
No
Check if the category consists large number of codes
Yes
Divide category into sub-category
No
Developing and testing hypotheses / propositions
Check any code can be discarded based on key theme
Yes
Set Not Applicable for respective comments with rationale
Updated list of code with key theme
No
Develop the hypotheses / propositions for each code based on the key theme
Test the credibility of developed hypotheses / propositions
If an alternative hypothesis can derive for a code
Yes
Review the hypothesis explanation and revisit the developement process of respective code and key theme
No
End

Figure 3-2: Methodology for analysing interview response

The preparation stage involved recording all the interview response comments and the researcher familiarising themselves with the comments. The preparation stage involved the following steps:

1) Record all the comments in a spreadsheet for better visualisation and for ease of analysis, as the participant organisation sent the response electronically in Word format;
2) Read each of the comments and check whether any clarification is required. It was found that no further clarification was needed.

The **categorisation** stage involved creating initial categories based on the interview objective, research question, and aim of the research, which resulted in the following three categories:

1) **Methodological challenges** – comments related to the challenges in integrating security identification, analysis, testing, and monitoring in their development methodology
2) **Organisational challenges** – comments related to the challenges arise due to the company's policies, factors about market and external stakeholders
3) **Technical challenges** – comments related to specific security and privacy concerns when designing and implementing WBAN applications

Unitising data involves creating units of data from the comments and attaching it to an appropriate category. A unit of data may be a number of words, a transcript line, a sentence, several sentences, a complete paragraph, or some other chunk of textual data that fits the category. Unitising data involved carefully reading the comments several times, each time underlining the content that applied to any sub-category and annotating the underlined content with the sub-category code. This process was repeated until no new text for coding emerged. During this step, a total of 15 units of code were produced. As an exemplar, Table 3-2 illustrates the sub-category and unit of data creation for the technical challenges category.

Table 3-2: Illustration of technical challenges category sub-category and unit of data

Category	Unit of Data	Code	Sub-category
Technical Challenges	Architectural consideration of security at sensor, network, application and data storage level	Arch_Design_Con	Architectural Design and Data Flow
	Understanding the data flow around their system and what assets need to be protected	Data_Flow	
	Indentifying security and privacy risk control	Ind_Sec_Risk_Con	Security and privacy risk control
	Security and privacy risk control implementation details	New_Sec_Con_Source	
	Security and privacy mechanisms for sensor nodes, which are often limited by physical memory constraints, computational powers and storages	Sec_Con_Selection_Pro	

The next step, **recognising relationships and developing the categories** involved organising the list of codes with their respective categories followed by checking whether the key theme or concepts are recurring in the code. If the concept is recurring, then merge the matching codes. Additionally, check if any categories consist of a large number of codes, then divide the category into a sub-category and attach the appropriate code. As part of this step, a total of 8 subcategories were produced.

The developing and testing propositions stage involved creating the hypothesis or proposition for each code. Once the proposition was developed for each code, a focus group was set up to review the creditability of the proposition. In this research study, the focus group consisted of two members from the RSRC having extensive expertise in the area of security and privacy for medical devices. The focus group members reviewed each proposition to reach a consensus to address the comments. In cases where focus group members were unable to reach a consensus for a proposition, revisit the development process of the respective code and key theme and update the proposition. The findings from this step are outlined in the next section.

3.4 Findings

3.4.1 Methodological Challenges

The interviewee faced methodological challenges in integrating security identification, analysis, testing, and monitoring in its development methodology. In response to the question *"Do you face any challenges to incorporate the security and privacy requirements in your software development process?"*, the interviewee stated that they have very limited experienced staff to implement standards guideline in their existing software development process. The interviewee also stated that top management is reluctant to provide the necessary support, budget and resources for implementing a standard.

Interviewee also mentioned that while reviewing the security and privacy standards, they found each standard consists of a vast number of controls. This vast number of controls raises the challenge of prioritising the control while preparing the release plan. Furthermore, the organisation also found that the standards typically provide a high-level outline of each security and privacy control without giving sufficient detail on how to implement the control. While this can be useful for providing a comprehensive overview of the security and privacy landscape, it can also make it challenging for the organisation to know exactly how to implement each control effectively. The organisation thinks they need to onboard experienced security and privacy experts who can help them translate the standard's requirements into specific implementation details and best practices. Below is the list of methodological challenges identified from the interview:

- Lack of trained staff, budget, and management support
- Due to a vast number of controls, the challenge is prioritising these controls in addition to planning releases without compromising security and privacy

- Standards outline each security control at a very high-level with limited amount of implementation details

3.4.2 Organisational Challenges

Organisational challenges can arise from a variety of factors, such as a company's policies, market conditions, and external stakeholders. Regarding the question about the regulatory compliance, Interviewee mentioned that the organisation plans to incorporate regulatory compliance related to the US and EU markets into the WBAN application. They specifically mentioned regulatory compliance, such as HIPAA, and GDPR. Their limited knowledge about market-specific regulatory requirements, standards, and policies, poses a significant challenge for incorporating security and privacy into the application. They also think the company must stay up-to-date with the latest regulations and security standards relevant to the HIPAA, and GDPR to avoid compliance issues and potential security breaches. The organisation also mentioned that they face another challenge regarding the existing standards, that is market-specific regulatory requirements are complex and difficult to implement. They also think they need to seek expert guidance and resources to help them implement these standards effectively. Below is the list of methodological challenges identified from the interview:

- Limited knowledge about market-specific regulatory requirements, security standards, and policies
- The existing standards are too complex and complicated to implement

3.4.3 Technical Challenges

Technical challenges can arise when designing and implementing Wireless Body Area Network (WBAN) applications, particularly when it comes to assuring security and privacy. Understanding the data flow around a system is crucial in identifying potential vulnerabilities and ensuring that adequate security measures are implemented. It involves analysing how data is collected, processed, stored, and transmitted within the system and identifying all the assets that need to be protected. Assets can include hardware, software, network components, and data itself. By understanding the data flow and assets that need to be protected, security professionals can develop a comprehensive security strategy that addresses all potential risks and threats.

One of the biggest challenges for ensuring security and privacy in WBANs is the lack of a comprehensive understanding of the architecture for WBAN security and privacy. WBANs are designed to collect and transmit sensitive medical data, which makes them vulnerable to attacks and breaches. However, the architecture for securing WBANs is complex and involves multiple layers of security measures, including authentication, encryption, and access control. Without a comprehensive understanding of the architecture for WBAN security and privacy, it can be difficult to implement effective security measures and ensure that sensitive medical data is protected. Therefore, it is important to invest in research and development to better understand the architecture for WBAN security and privacy and develop effective solutions to address these challenges.

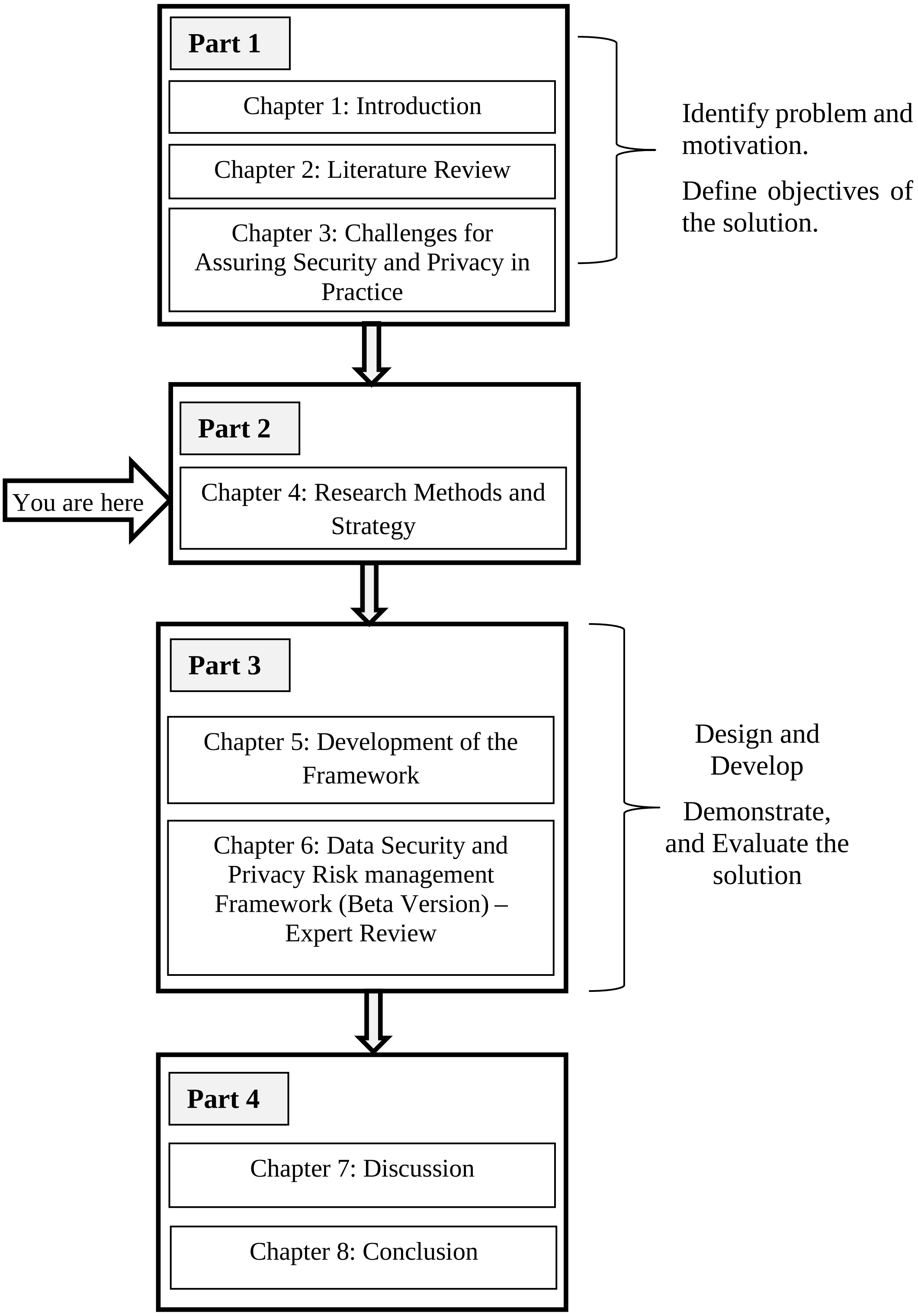
Another significant challenge in securing WBANs is the lack of security mechanisms for sensor device nodes connected to wireless networks. These devices are often limited by physical memory, computational power, and storage, which makes it difficult to implement comprehensive security measures. Furthermore, many of these devices are designed for specific medical applications, which can make it challenging to develop standardized security protocols that can be applied universally across all devices. As a result, many sensor device nodes are vulnerable to attacks and breaches, which can compromise the security of the entire network. Addressing this challenge requires developing security mechanisms that are tailored to the specific limitations of sensor device nodes, as well as implementing standards-based security protocols that can be universally applied across all devices. This will help to ensure that all devices connected to the network are protected and that sensitive medical data is secured. Below is the list of technical challenges identified from the interview:

- Understanding the data flow around the system and what assets need to be protected
- Lack of comprehensive understanding of the architecture for WBAN security and privacy
- Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage

3.5 Conclusion

The literature review indicates that adopting a cybersecurity framework is challenging due to various barriers that need to be overcome. It was found that there are six main challenges faced by organisations when trying to adopt a cybersecurity framework. During the interview, a total of nine challenges were identified for ensuring security and privacy. All six challenges identified in the literature review were also mentioned during the interview. The interviewee pointed out that reviewing security and privacy standards is challenging as each standard consists of a vast number of controls that need to be prioritised when preparing the release plan. Additionally, the interviewee mentioned facing difficulties in understanding the data flow and assets that require protection, which is essential in developing a comprehensive security strategy that addresses all potential risks and threats. Moreover, the interviewee also highlighted the challenge of securing WBANs due to a lack of comprehensive understanding of the architecture for WBAN security and privacy, which involves multiple layers of security measures such as authentication, encryption, and access control.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
You are here
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

4 Research Methodology

4.1 Introduction

There are many different research approaches and methods in empirical software engineering research. A challenge experienced by most researchers for empirical software engineering research is selecting which research method is most appropriate (Easterbrook *et al.*, 2008). Easterbrook *et al.* (2008) discussed that the pros and cons of research methods are not well documented and lack of knowledge about the implications of the methods they use makes it challenging to select the most appropriate research method. The type of research being performed will determine which research method is most suitable. This chapter presents a review of the principal philosophical approaches to research. A number of research methodologies are presented and reviewed in terms of their suitability for conducting and evaluating the research to achieve the research objectives of this work.

4.2 Research Paradigms

A research paradigm is a set of widely accepted beliefs and assumptions about ontological, epistemological, and methodological concerns within a research community. Alternatively, a paradigm can be defined as *"a particular worldview where philosophy and methods intersect to determine what kinds of evidence one finds acceptable"* (Patton, 2001). The research paradigm sets the direction in how the research will be carried out. There are two dominant research perspectives namely the Positivist and Interpretivist paradigms. These paradigms can be differentiated by their epistemology and ontology. Epistemology asks what knowledge is and how it can be obtained, and the degree to which it is possible to know about any particular subject. Ontology refers to our ideas about how the universe is made up and the meaning of things.

4.2.1 Positivism

Positivism is commonly considered a scientific approach with techniques used by the scientific community to study real-world behaviours. The basic assumption of Positivism is that the world is ordered and regular, and it can be investigated objectively (Oates, 2006). Saunders et al.(2009, pp.119) describe that positivist research is generally conducted in a controlled environment, and the researchers will often use observations as a data collection method. Positivism has the following characteristics:

- The world exists independently of humans
- Researchers use observations and measurements to develop hypotheses that will have one explanation, i.e. 'the truth'
- The researcher is an impartial observer and discovers the facts independently without researchers' personal values and beliefs
- The researcher uses empirical testing for confirmation or refutation of theories and hypotheses
- Often use mathematical modelling and statistical analysis of quantitative data to provide logical, objective means of analysing observations and results
- The research looks for generalisations of the facts which are true regardless of the researcher and the context

4.2.2 Realism

Realism is an ontological position, which assumes that reality exists independently of the researcher's perception (Khanna, 2018). As an example, a healthcare researcher will view the concepts of disease as *'things in the world'* independent of his or her perceptions. Braun and Clarke (2013, p.27) define that realism assumes a world of knowledge that can be understood through research, where the truth is *'out there'* and accessible through the proper application of research techniques. The authors also state that realism is the ontology that underlies most quantitative studies, but it rarely informs qualitative studies.

4.2.3 Interpretivism

Interpretivism explores how the factors in social settings are related and independent. Saunders et al. (2009, p.116) advocate that the researcher needs to understand the difference between humans in our roles as social actors. Interpretivism looks at how people perceive their world. Oates (2006) characterises interpretivism as that the researcher is not neutral, and they need to acknowledge how they influence the research. The author also states that reality can only be accessed or transmitted to others through social construction, such as language and shared meaning. Positivists criticise interpretivism for being non-scientific therefore, interpretivism has to assure their research is supported with data, e.g., interviews, questionnaires, observations and documents. Interpretivism has the following characteristics (Oates, 2006):

- No single version of the ‘truth’. Reality or knowledge is a construction of our mind, either individually or in a group. Different groups of people perceive the world differently
- Use socially constructed mediums such as language and shared meanings and understanding to access and transmit reality for an individual or a group
- Researchers must be intuitive or self-reflective to acknowledge how their interactions are going to influence the research
- The research aims to better understand people within their natural social settings, not in the artificial world
- Strong preference for generating and analysing qualitative data
- Researchers expect to propose several explanations for what happens in their research

4.2.4 Pragmatism

Pragmatism argues that the most important determining factor of research is the research question, and that both positivist and interpretivist viewpoints can be used (Saunders et al., 2009). Pragmatism is the philosophical underpinning of mixed methods research. Creswell et al. (2018) identify the following key characteristics for pragmatism:

- Pragmatism is not committed to any one system of philosophy and reality
- Individual researchers have freedom of choice
- Pragmatists do not see the world as absolute
- Truth is what works at the time
- Pragmatist researchers look to the 'what' and 'how' to research based on its intended consequences
- Pragmatists agree that research always occurs in social, historical, political, and other contexts

This study involves interviews and trials in organisations. It uses both qualitative and quantitative methodologies. This mixed-method research is supported by pragmatism.

4.3 Research Approach

The research approach is a plan and procedure that consists of the details, steps, and methods used for data collection and analysis. When designing a research project, the researcher needs to consider the appropriate research approach which will be used to carry out the research. Saunders et al. (2009, p.124) presented two research approaches, which are an inductive and a deductive approach. In an inductive approach, data is collected first, and then a theory is developed by analysing the data. A theory and hypotheses are developed in the deductive approach, and then a research strategy is developed to test the hypotheses. In Table 4-1 below, Saunders et al. (2009) present several significant differences between the deductive and inductive approaches.

Table 4-1 Differences between Inductive and Deductive approach

Deductive approach	Inductive approach
• Scientific principles • Moving from theory to data • The need to explain causal relationships between variables	• Gaining an understanding of the meanings humans attach to events • A close understanding of the research context • The collection of qualitative data

Deductive approach	Inductive approach
• The collection of quantitative data • The application of controls to assure the validity of data • The operationalisation of concepts to assure clarity of definition • A highly structured approach • Researcher independence of what is being researched • The necessity to select samples of sufficient size to generalise conclusions	• A more flexible structure to permit changes of research emphasis as the research progresses • Less concern with the need to generalise

Although both approaches are distinct and mutually exclusive, both approaches can be used in conjunction with each other. This study takes both an inductive and deductive approach into account while designing the research. Initially, an inductive approach is taken to gather information and the theory developed (WBANSecRM framework to assure security and privacy). A deductive approach is then taken to prove this theory, the WBANSecRM framework was developed and trialled in test bed organisations.

4.4 Research Choices

Research methods are the tools or techniques used to gather data. There are two methods that can be used in data collection, qualitative and quantitative methods.

Qualitative research is a process in which data collection and analysis techniques emphasise generating or using non-numerical data. This process explores attitudes, behaviours and experiences. The qualitative research process is generally inductive rather than deductive, which generates theory from the interpretation of the evidence (Spratt et al., 2004). Action research, observation, interviews, ethnography, and grounded theory are examples of qualitative methodologies.

Quantitative research is described as any data collection technique or data analysis procedure that produces and utilises numerical data (Saunders et al. 2009). Quantitative research places the emphasis on measurement while collecting and analysing data. The researcher can use a large-scale survey to collect data and generate a statistical report from the data. Quantitative research is more suitable when the research requires the measurement of variation and diversity. Generally, it uses the deductive approach to draw a hypothesis from a theory. Examples of methods used in quantitative research include questionnaires, surveys, interviews, experiments, case studies, content analysis and observations.

In a research project, the researcher can use either a qualitative or a quantitative approach , or a combination of both within the same project (Crotty, 1998). Using a single data collection and analysis approach in a research project is known as *'Mono methods'*. The combination of qualitative and quantitative methods is known as *'Multiple methods'* (Saunders et al. 2009). Multiple methods can be further divided into two more categories named *'Mixed-method'* and *'Multi-method'*. Figure 4-1 outlines the categorisation of research choices.

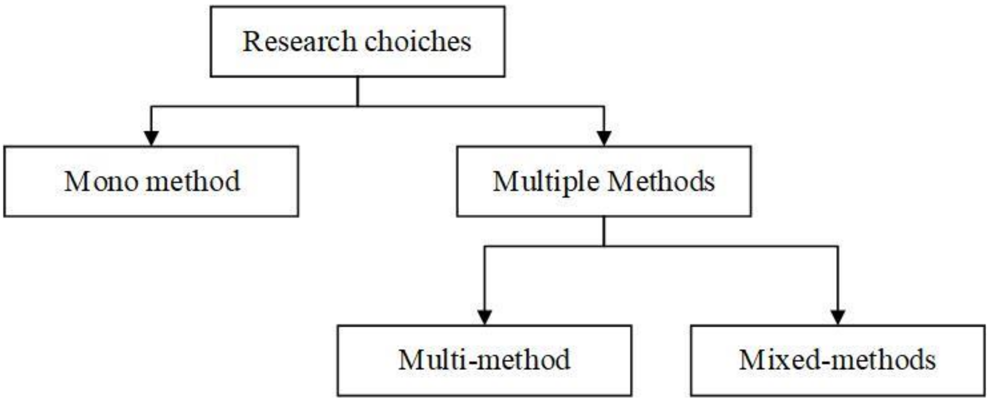


Figure 4-1: Research Choices

Multi-method occurs when more than one data collection technique and analysis process is used, but these techniques must be all quantitative techniques or else all qualitative techniques. Mixing the qualitative and quantitative techniques is known as *'Mixed methods'*. The use of multiple approaches in a single research project can capitalise on each approach's strengths and offset its weaknesses. Multi-method designs are usually intended to supplement one source of information with another or 'triangulate' on an issue using various data sources to address a research problem from different points of view. Mixed-method design is conceptually more complex and involves different ways of conceptualising the problem.

This study uses the mixed-method approach for the following two reasons:

1) Data is collected qualitatively by conducting interviews in one company, and it is collected both quantitatively and qualitatively through assessment of the framework
2) Data triangulation and method triangulation corroborates the results of the literature review, organisational interviews, expert review, and industrial pilot in a WBAN based application development organisation. This triangulation gives greater overall confidence in the study

4.5 Research Strategies

A research strategy is an overall plan of action for conducting the research study. A research strategy guides researchers in planning, executing, and monitoring the research study. The research strategies considered in this section are Ethnography, Case Studies, Grounded Theory, Action Research (AR), Design Research (DR) and Action Design Research (ADR).

4.5.1 Ethnography

Ethnography is a systematic approach to studying communities' social and cultural lives (LeCompte et al., 1999). The main aim of the ethnography approach is to provide a holistic insight into people’s views, actions, and the nature of the location they inhabit. Ethnography usually involves the researcher integrating and living with participants for long periods. Ethnography is not suitable for this research as the development of the risk management framework does not require the researcher to have close interaction and observation of participants for long periods.

4.5.2 Case Study

Case study is a research strategy that involves an empirical investigation of a particular phenomenon within its real-life context (Robson and McCartan, 2016, p150). Case studies focus on understanding a specific phenomenon in context using examination and observation. This study focuses on developing a risk management framework that can be used across different medical device organisations (not a single context). Hence, the case study is not a suitable research strategy for this research.

4.5.3 Grounded Theory

Grounded theory is a research strategy used to develop a theory by analysing the material or studying a field or process (Flick, 2018, p.538). Researchers are responsible for developing the theory by observing a group. Saunders et al.(2009, p.142) propose to use a combination of inductive and deductive approaches to develop the theory. The grounded theory approach was not considered appropriate for this research. This research does not aim to create a theory but rather aims at developing a solution by addressing the research questions that have been developed early in the research process.

4.5.4 Action Research

Action research (AR) is a research methodology where the researchers collaborate with a group of people to improve a situation or solve a problem in a particular setting (Dawson, 2019, p.17). The author also states that in AR, "*the researchers do not 'do' research 'on' people; instead, researchers work with them and act as a facilitator*". A range of activities is required which focus on research, planning, theorising, learning and development. AR requires a continuous research and learning process that builds a long-term relationship with a problem (Cunningham, 1993). AR is essentially a change-oriented approach in which complex processes are studied by introducing change and observing the effects (Baskerville, 1999). Given (2008, p.4) states a total of five overlapping cycles are involved in AR which are illustrated in Figure 4-2. These cycles are investigation, action planning, piloting of new practices, evaluation of outcomes, and incorporating at all stages the collection and analysis of data and the generation of knowledge.

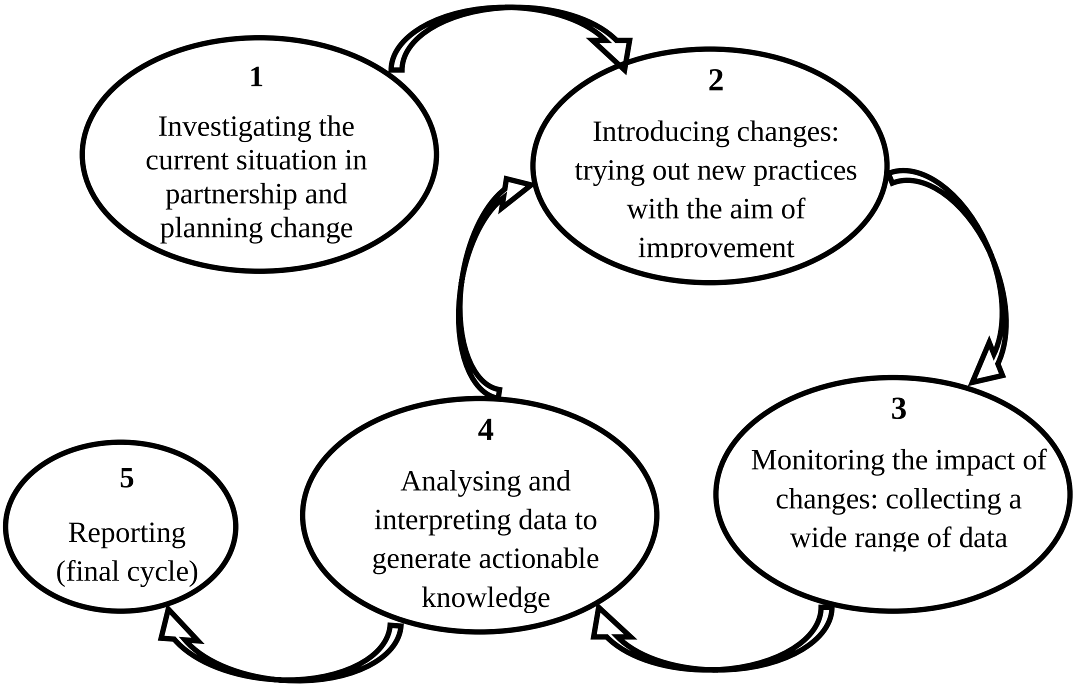

1
Investigating the current situation in partnership and planning change
2
Introducing changes: trying out new practices with the aim of improvement
3
Monitoring the impact of changes: collecting a wide range of data
4
Analysing and interpreting data to generate actionable knowledge
5
Reporting (final cycle)

Figure 4-2: Model of Action Research (Given, 2008)

The goal of AR is to find the solution to a practical problem while simultaneously contributing to scientific theory. Maintaining a balance between the goals of the researcher and the goals of the organisation must be achieved. AR creates a bridge between the practitioner and the generation of theoretical knowledge. The role of the researcher and practitioner are presented in Table 4-2.

Table 4-2: Different role of actors in Action Research during three phases of research (Järvinen, 2012)

	Researcher	Practitioner
In the beginning	Non-dominant	Dominant
During the real process	Collaborative	Collaborative
At the end	Dominant in scientific evaluation	Dominant in practical evaluation

This research method is very popular in areas such as organisational management, community development, education and agriculture (Dawson, 2019, p.17). AR was not suitable for this study as the researcher will have the dominant role during the three stages of the research. The researcher will develop the security and privacy risk management framework (dominant in the beginning), and the researcher will also oversee the validation through expert reviews (dominant) and implement it in the host organisations (collaborative). Furthermore, AR is most suitable for solving a particular problem within an organisation but is not suitable for developing a framework for generic use. This research aims to develop a data security and privacy risk management framework for WBAN based healthcare applications that will not be limited to a particular company setting.

4.5.5 Design Research

Design research (DR) is a methodology used for building and evaluating IT artefacts. It intends to solve a class of problem. The outcome of DR not only provides a new innovative artefact, it also helps develop knowledge about creating another artefact which belongs to the same class. Hevner *et al.* (2004) define design research as "*The design-science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts*". March and Smith (1995) outlined two main processes of DR, that is 'build' and 'evaluate'. Hevner *et al.* (2004, p.75) also states that, the DR framework is '*knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artefact*'. These two processes (build and evaluate) are used to design the artefacts, which will fulfil the business need. March and Smith (1995) also identified four possible outputs for DR; 1) *construct*, 2) *models*, 3) *methods*, and 4) *instantiation*.

Peffers *et al.*(2007) states that the slow adoption of DR in Information Systems is due to *'the lack of a methodology to serve as a commonly accepted framework for DR and of a template for its presentation'*. To address that issue the authors proposed and developed a design science research methodology (DSRM). Peffers *et al.*(2007) also introduced a six step process for DR:

1) Problem identification and motivation
2) Define the objectives for a solution
3) Design and development of a solution

4) Demonstration through experimentation, simulation, case study, proof, or other appropriate activity
5) Evaluation - comparing the objectives of a solution to actual observed results from use of the artefact in the demonstration
6) Communication - communicate the problem, its importance, and the solution to researchers and practising professionals

Järvinen (2012) identify the role of the researcher and practitioner in DR based on:

a) Whether the researcher or the practitioner is the originator of the research process
b) How they cooperate during the research process
c) How rigor and relevance are applied

The role of the researcher and practitioner in DR during the three phases of the research are presented in Table 4-3.

Table 4-3: Different role of actors in Design Research during three phases of research (Järvinen, 2012)

	Researcher	**Practitioner**
In the beginning	Dominant	No Involvement
During the real process	Dominant	Non-dominant
At the end	Dominant in scientific evaluation	Dominant in practical evaluation

DR assumes neither any specific client nor joint collaboration between researchers and the client while carrying out the research (Iivari and Venable, 2009). The roles presented in Table 4-3 also reflect that the practitioner plays a non-dominant role during the real process phase of the research. In this study, the researcher requires collaborative support from the practitioner to develop and review the WBANSecRM framework during the framework's development phase. Existing DR methods focus on building the artefact and relegate evaluation to a subsequent and separate phase. The build and evaluate DR processes do not meet the rigorous cycles and organisational intervention needs for designing artefacts (Sein *et al.*, 2011). The author also concluded the DRSM DR model developed by Peffers *et al.*(2007) does not recognise the artefacts materialisation within the interaction of the organisational elements.

Cole *et al.*(2005) also states that DR methods are useful for supporting abstractions and invention, but they consider organisational intervention secondary. DR method is inappropriate for this research, as design, development and review of the WBANSecRM framework require decisive organisational intervention with rigorous cycles.

4.5.6 Action Design Research

Action Design Research (ADR) is a cross-fertilisation of AR and DR. It provides guidelines for building, intervention, and evaluating a research strategy. The ADR methodology was developed to facilitate a useful approach to benefit the interests of both information system research and organisational research (Cole *et al.*, 2005). Sein *et al.*, (2011) define ADR as *"a method that focuses on the building, intervention, and evaluation of an artefact that reflects not only the theoretical precursors and intent of the researchers but also the influence of users and ongoing use in context".* The authors also describe the ADR methodology as supporting the inclusion of the evaluation stage in DR when building the artefact, rather than the relegation of this phase to a subsequent and separate stage. ADR consists of four stages and principles presented in Figure 4-3.

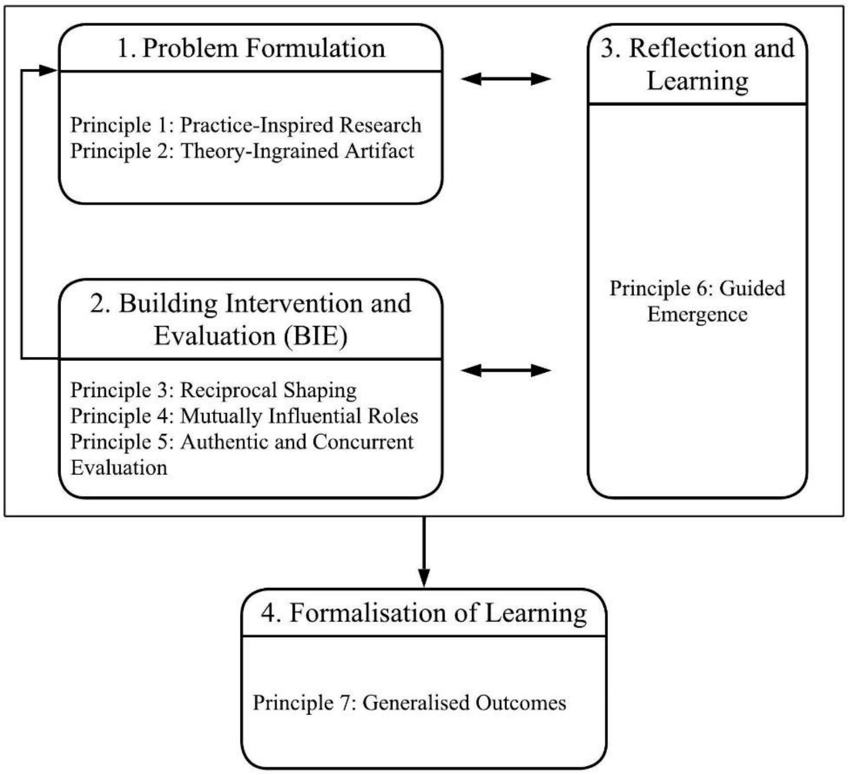

1. Problem Formulation
Principle 1: Practice-Inspired Research
Principle 2: Theory-Ingrained Artifact
2. Building Intervention and Evaluation (BIE)
Principle 3: Reciprocal Shaping
Principle 4: Mutually Influential Roles
Principle 5: Authentic and Concurrent Evaluation
3. Reflection and Learning
Principle 6: Guided Emergence
4. Formalisation of Learning
Principle 7: Generalised Outcomes

Figure 4-3: Stages and principles of action design research method (Maung K. Sein *et al.*, 2011)

Stage 1 Problem formulation:

The initial phase of ADR is problem formulation, which provides an opportunity to identify and conceptualise the problem. The problem can be identified based on existing theories, technology, or organisational perception (Sein *et al.*, 2011). The problem formulation stage is based on the two principles of Practice-Inspired Research and Theory-Ingrained Artefact. Practice-Inspired Research emphasises the use of field problems as a knowledge creation opportunity, while Theory-Ingrained Artefact is used to create and evaluate an artefact informed by theories.

Stage 2 Building Intervention and Evaluation (BIE):

The second stage of ADR involves taking the output from Stage 1 and generating the initial design of a solution artefact. The initial artefact, which consists of implementation details for security and privacy controls, was shaped by conducting multiple interviews with a company. The result of the BIE stage is the final design of the artefact. There are two approaches in BIE:

- Organisation-Dominant BIE: Organisation-dominant BIE is suitable in situations where organisational intervention is a primary source of innovation to generate design knowledge. This approach to BIE deploys the artefact in the organisation early in the design process. During the iterative process, the ADR team consisting of the researcher, practitioner and end-user can challenge the organisation participants about specific ideas and assumptions of existing artefacts. This iterative process helps to create or improve the artefact design. The iterative process will stop when an organisation decides to adopt or reject the artefacts, and/or design changes are very marginal.
- IT-Dominant BIE: IT-Dominant BIE is when the artefact is developed by researchers with large contributions from practitioners. It commences with designing the alpha version of the artefact, which is usually developed without input from an organisation. Then, the artefact is continuously refined through organisation intervention. This iterative process involves engagement between the researcher and practitioners and helps to build and reshape the artefact.

Stage 3 Reflection and learning: The reflection and learning stage helps to apply the knowledge gathered from stages 1 and 2 to build a solution that can apply to a broader class of problems. Stage 3 is an iterative process that is conducted in parallel with stages 1 and 2. The principle at this stage is guided emergence. The collaborative artefact will replicate the preliminary design developed by the researchers and its ongoing formation through organisational engagement.

Stage 4 Formalisation of Learning: The final phase of the ADR process is Formalization of Learning. This phase of the research process is concerned with assuring that ADR provides the ability to generalise learnings, meaning that the solution is applicable in a range of contexts.

ADR helps researchers to make a significant scientific contribution while at the same time assisting in solving practitioner problems. ADR involves developing collaborative artefacts in the technological and organisational context and shaping the artefacts within a dynamic and flexible development environment. ADR promotes the technical rigour in artefact development, but not at the cost of organisational relevance. ADR is the chosen strategy for this research for the following reasons:

- The researcher identified and formulated the problem by executing the literature review and interviews
- Given the nature of this research and the nature of threats and vulnerabilities in WBAN applications, artefact development required close collaboration with organisations
- ADR allowed the researcher and practitioner to collaborate using a rigorous iterative cycle during the early stage of the development of the WBANSecRM framework
- The researcher produced an artefact in the form of a framework that validated in the context in which it will be used
- The outcome of this study produced a generalised version of the artefact

4.6 Application of Action Design Research

This section presents each of the ADR stages and associated principles and discusses how and why they are applied in this study.

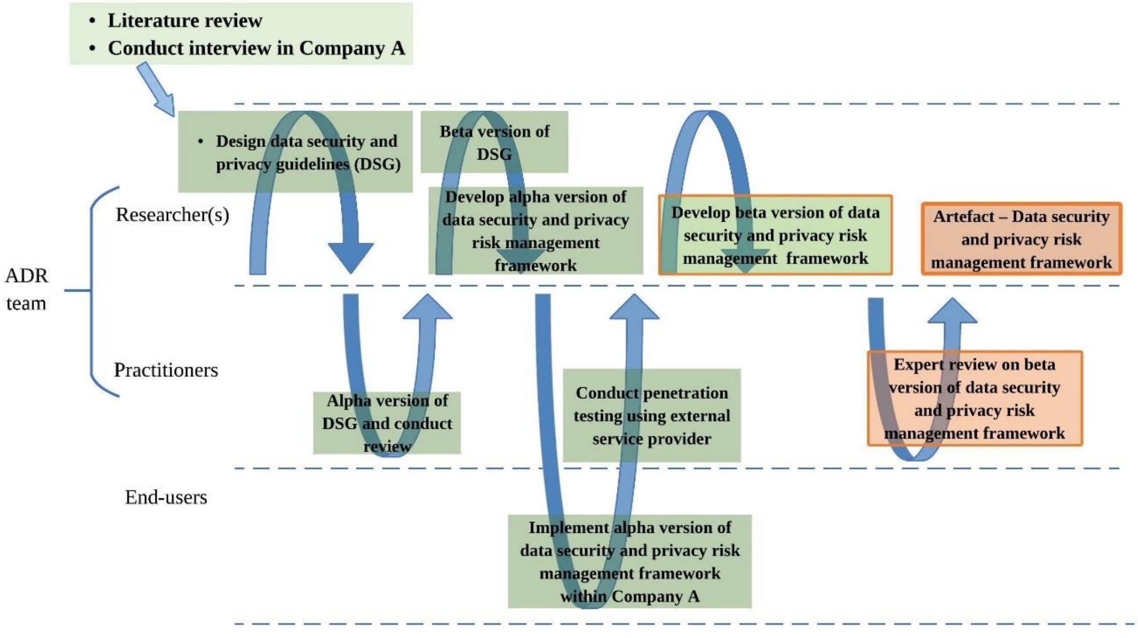
Stage 1 Problem formulation:

In this research, the problem was initially identified through one organisation's request for guidelines for assuring data security and privacy in their fitness tracking application. This research problem was further defined and conceptualised through an interview conducted with the organisation to identify the challenges faced by developers in assuring data security and privacy. The interview resulted in developers needing extensive knowledge about the attacks, threats, vulnerabilities, and security and privacy requirements for WBAN based healthcare applications. Furthermore, a structured literature review was conducted based on the results of the interview to identify the attacks, threats, vulnerabilities, and security and privacy requirements. The findings from this literature review were then published (Paul *et al.*, 2019).

Additionally, a literature review was also conducted to identify the existing frameworks, methods, and techniques used to assure data security and privacy of WBAN based healthcare applications. An analysis of these frameworks, methods and techniques revealed that none of them fully addressed all of the previously identified challenges.

Stage 2 Building Intervention and Evaluation (BIE):

This research adopted the IT-Dominant BIE approach as the initial framework will be designed outside of the organisational context. The artefact will then be iteratively reviewed and piloted in an organisational setting. An illustration of the IT-Dominant BIE approach used during this research is presented in Figure 4-4. At the BIE stage, the ADR team consisted of a combination of the researcher and practitioners. The practitioner team included a chief technical officer, a technical lead and a senior developer from the organisation henceforth known as Company A. The end-users are the organisation's software development team. The senior developer played a dual role as both practitioner and end-user. The researcher worked closely with the practitioner group to design and evaluate the design artefact in an iterative process. Figure 4-4 represents how the WBANSecRM framework evolved throughout the iterative process.



• Literature review
• Conduct interview in Company A
• Design data security and privacy guidelines (DSG)
Beta version of DSG
Develop alpha version of data security and privacy risk management framework
Develop beta version of data security and privacy risk management framework
Artefact – Data security and privacy risk management framework
ADR team
Researcher(s)
Practitioners
End-users
Alpha version of DSG and conduct review
Conduct penetration testing using external service provider
Expert review on beta version of data security and privacy risk management framework
Implement alpha version of data security and privacy risk management framework within Company A

Figure 4-4: BIE diagram for developing a data security framework

As illustrated in Figure 4-4 an alpha version of the data security guidelines (DSG) was developed by the researcher after conducting a literature review and an interview with Company A. The alpha version of the DSG consists of a data flow diagram of the application and the guidelines to implement security and privacy controls. The practitioner group reviewed this alpha version of the DSG. A beta version of the DSG was developed, taking into account feedback from the review. The implementation details for each security and privacy control of the DSG beta version are presented in Appendix C. The beta version of the DSG was then used to create an alpha version of the data security and privacy framework. During the implementation phase the researcher worked closely with the development team to collect feedback about the usability and effectiveness of the WBANSecRM framework. When the development team completed the implementation of the alpha version of the WBANSecRM framework, the organisation's fitness tracking application was then tested by an external penetration testing organisation. The goal of on-boarding a penetration testing team was to test the application from a security and privacy perspective. The penetration test also helped to determine the efficacy of the security and privacy controls proposed by the WBANSecRM framework. All feedback from the penetration testing and development team was collected and analysed, and necessary modifications were made to the alpha version of the WBANSecRM framework. These changes resulted in the beta version of the WBANSecRM framework. As the primary goal of this research is to develop a data security and privacy framework for WBAN based healthcare applications, this research intends to demonstrate the generalisability of the WBANSecRM framework in stage 3 and stage 4.

Stage 3 Reflection and learning: The design and redesign of the WBANSecRM is reflected upon by the researcher based on the feedback received from practitioners, including expert reviewers and end-users. This reflection assures that the artefact (WBANSecRM) adheres to the design principles by assuring that the artefact has absorbed the organisation specific learnings and has expanded the learnings from the specific context to assure applicability to a broader class of problems. This involves the iterative evaluation of WBANSecRM by the experts/practitioners from academia and industry.

Stage 4 Formalisation of Learning: Any solution must be generalisable and can then be tailored for use by any organisation developing WBAN based healthcare applications regardless of size or geographical location. The formalisation of learning phase also involves publishing and communication of the research outcomes. The WBANSecRM was published as a research paper and made available to practitioners. In addition to the publication of the WBANSecRM, a number of papers have been published in relation to the development and use of the WBANSecRM. These papers are listed in the publications section at the beginning of this thesis (Publications).

4.7 Data Collection Methods

The data collection methods considered in this section are document analysis, surveys and observation.

Document analysis is a systematic procedure for reviewing and evaluating documents in order to identify the presence of a certain text or a concept, by reading, skimming and interpretation. In qualitative research, document analysis helps to identify and elicit meaning, gain understanding and develop empirical knowledge about a concept (Bowen, 2009). This type of data collection method is suitable for this research, in particular, to identify the challenges faced by the organisation to assure security and privacy and to compile lists of assets with respective threats and vulnerabilities. Furthermore, this method is also suitable for analysing the security and privacy requirements and controls from various medical device regulations and their respective standards and guidelines.

Surveys are a data collection method that use a predefined group of people or organisations to gain information and insights into various topics of interest. Surveys are an excellent approach to collect large amounts of data from a sample population and to provide a broad and representative perspective from the whole population. A survey can be conducted and administered electronically, or by face-to-face interview. Since this research is concerned not only about what data security and privacy challenges an organisation is faced with but also about how the organisation should address these challenges, a semi-structured interview was used to identify the challenges faced by the organisation in assuring security and privacy for a WBAN based application. Additionally, a semi-structured interview was used to collect feedback and suggestions after implementing the alpha version of the WBANSecRM framework. Furthermore, a survey was used to collect data from expert reviews to identify the usability and efficacy of the WBANSecRM.

Observation entails the '*recording (field notes) of events, behaviours and artefacts in their social setting*' (Saunders et al., 2009, p.288) and is fundamentally qualitative in its approach. There are two types of observation which are participant observation and structured observation (Saunders et al., 2009, p.282). Participant observation is a type of qualitative observation and structured observation is a type of quantitative observation. Participant observation enables the researcher to directly observe the events and/or participate in the activities studied in the research setting. Structured observation is a type of quantitative observation that focuses on the frequency of certain acts (Saunders et al., 2009, p.288). Structured observation normally necessitates the researcher spending a significant amount of time in the setting. However, gaining access to organisations for such a period of time can be problematic. This study aims to assist organisations in assuring security and privacy; observing the participant behaviour while developing the application will not help to assure security and privacy. For these reasons, observations were not thought suitable for this research.

4.8 Summary of Methods, Strategies and Choices

An overview of the path taken in this study in terms of philosophy, approach, choices, strategies and data collection techniques is presented below in Table 4-4. This study involves interviews and organisational trials, which includes the use of both qualitative and quantitative methodologies. This mixed-method research is supported by the pragmatic philosophical perspective advocated in this study.

Table 4-4: Overview of Research Process

Research Philosophy	Research Approach	Research Choices	Research Strategies	Data Collection
Pragmatism	Inductive/Deductive	Mixed Methods	Action Design Research	Surveys, Document Analysis

During the research design, this study considers both an inductive and deductive approach. Initially, an inductive approach was taken to gather information and develop a theory about how the development of a risk management framework can assist the organisation in assuring the security and privacy of WBAN based healthcare applications. Furthermore, a deductive approach was taken to prove this theory, as the WBANSecRM framework was developed and tested in an organisational setting. The mixed-method approach was used in this study as data was collected qualitatively through organisation interviews and then quantitatively and qualitatively through the expert review of the WBANSecRM framework.

AR is most suitable for solving a particular problem within an organisation but is not suitable for developing a framework for generic use. This research aims to develop a data security and privacy risk management framework for WBAN based healthcare applications that will not be limited to a particular company setting. DR methods are useful for supporting abstractions and invention, but they consider organisational intervention secondary. DR method is inappropriate for this research, as design, development and review of the WBANSecRM framework require decisive organisational intervention with rigorous cycles. So, the overall research strategy chosen for this study is ADR. ADR allowed the researcher and practitioner to collaborate using a rigorous iterative cycle during the early stage of the development of the WBANSecRM framework. Additionally, using ADR the outcome of this study produced a generalised version of the artefact. In addition, this study selected document analysis and survey as suitable data collection methods. Document analysis is suitable for this research for analysing the security and privacy requirements and controls from various medical device regulations and their respective standards. Finally, surveys are thought to be a suitable data collection method, as this study conducted interviews with Company A to understand the difficulties they were having in assuring security and privacy, and also to gather their feedback with regard to the efficacy and usability of the WBANSecRM framework throughout its' development. Additionally, a survey was conducted with a group of experts to determine the usability and efficacy of the WBANSecRM framework.

4.9 Action Design Research Applied

This section outlines how this study's objectives and research sub-questions were addressed using the ADR methodology. Figure 4-5 is a graphical representation of how ADR is applied in this study.

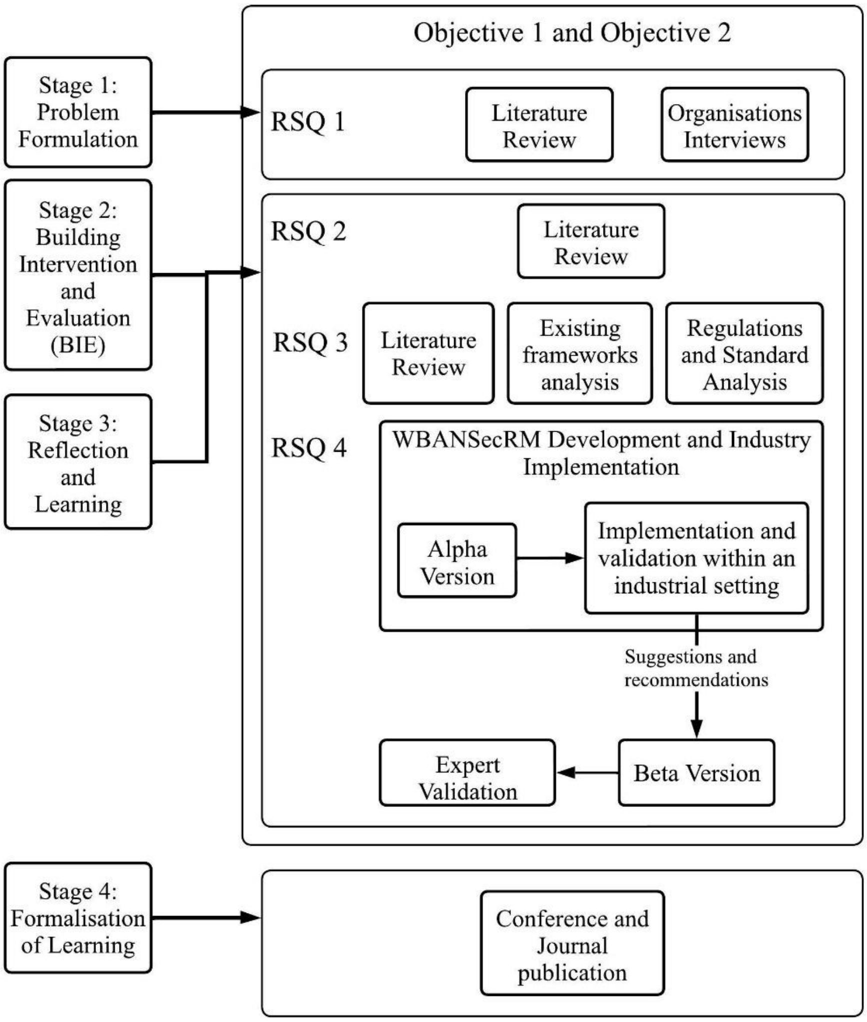

Objective 1 and Objective 2
Stage 1: Problem Formulation
RSQ 1
Literature Review
Organisations Interviews
Stage 2: Building Intervention and Evaluation (BIE)
RSQ 2
Literature Review
RSQ 3
Literature Review
Existing frameworks analysis
Regulations and Standard Analysis
Stage 3: Reflection and Learning
RSQ 4
WBANSecRM Development and Industry Implementation
Alpha Version
Implementation and validation within an industrial setting
Suggestions and recommendations
Beta Version
Expert Validation
Stage 4: Formalisation of Learning
Conference and Journal publication

Figure 4-5: Action design research applied to this research

The two objectives of this study are to:

- Design and develop the WBANSecRM which will assist developers in assuring security and privacy of WBAN based healthcare applications
- To validate the WBANSecRM

To meet these objectives, the following four research sub-questions were identified:

RSQ 1: What challenges are faced by developers of wireless body area network applications in assuring the security and privacy of PHR data?

RSQ 2: What frameworks, methods and techniques are used to assure data security and privacy for wireless body area networks?

RSQ 3: What should a WBANSecRM contain to assist wireless body area network application developers in assuring security and privacy and put them on the path to regulatory compliance?

RSQ 4: To what extent can the WBANSecRM address the challenges faced by developers in assuring data security and privacy while developing WBAN based healthcare applications?

The first stage of the action design research methodology provides answers to RSQ 1 and RSQ2. A literature review and an interview with a WBAN development organisation were performed to identify the challenges faced by the developer and organisation for assuring security and privacy. Additionally, the literature review and organisation interview also revealed that the solution should not be complex and should not require additional trained resources to implement the safeguards for assuring security and privacy.

The second and third stage of the action design research methodology answers RSQ2, RSQ 3 and RSQ 4. To answer RSQ 2, a literature review was conducted to identify the existing frameworks, methods, and techniques used to assure data security and privacy of WBAN based healthcare application. An analysis of those frameworks, methods and techniques revealed that none of them fully addressed the challenges identified in RSQ 1. Additionally, the analysis also revealed that these approaches only partially assure security and privacy, but none of them provide any guidelines to help put the organisation on the path to achieving regulatory compliance.

An analysis was conducted to identify security and privacy requirements from various healthcare legislations. Furthermore, a review of international security and privacy standards was conducted to identify the controls to fulfil the regulatory compliance requirements from a security and privacy perspective. The alpha version of the WBANSecRM was created, which was subsequently refined based on the suggestions and feedback received from the implementation within an industrial setting. The feedback received after the alpha version's industrial trial resulted in the beta version of the WBANSecRM framework. To evaluate the usability and efficacy of the beta version of the WBANSecRM, an expert review was conducted with a combination of experts from both academia and industry.

Finally, stage 4 of the ADR methodology is the Formalization of Learning, which resulted in the gamma version of the WBANSecRM which can be tailored to any organisation developing WBAN based healthcare applications regardless of size or geographical location. Producing the generalised version of the WBANSecRM requires more validation by implementing the gamma version of the WBANSecRM framework in multiple organisations with different sizes and locations. This research was unable to produce a generalised version of the WBANSecRM due to having limited access to WBAN application development organisations. The formalisation of the learning phase also involves presenting results and communicating the research outcomes. The WBANSecRM framework has been published as a research paper and made available to practitioners in this area. In addition to the publication of the WBANSecRM, a number of papers have been published in relation to the development and use of the

WBANSecRM. These papers are listed in the publications section at the beginning of this thesis (Publications).

4.10 Research Quality

The word *'quality'* is hard to define, and there are no absolute criteria to judge it, however criteria exist to differentiate good and poor quality. Reliability and validity are common criteria for evaluating qualitative and quantitative research (Braun and Clarke, 2013, p.278) (Golafshani, 2003). The following section details how reliability and validity are addressed throughout this research study.

4.10.1 Reliability

Reliability is concerned with the extent to which the results of a study or a measure are repeatable by a different researcher or in different circumstances. Reliability can be assessed by posing the following three questions (Easterby-Smith et al., 2012):

1. Will the measures yield the same results on other occasions?
2. Will other observers reach similar conclusions?
3. Is there transparency in how sense was made from the raw data?

Every effort has been made to include the instrumentation and protocols used in this study and to present a clear chain of evidence explaining how this research has been conducted. To safeguard the reliability of this research, the WBANSecRM framework produced in this study was developed based on the guidelines provided by AAMI TIR 57. AAMI TIR57 is a widely used risk management framework that guides the developer to perform information security and privacy risk management to address security and privacy risks within the medical device domain. To evaluate the alpha version of the WBANSecRM framework a penetration test was conducted with the help of a third-party penetration service provider. Furthermore, this study also documented the comments received during the expert review phase and how those comments were incorporated in the next version of the WBANSecRM framework.

4.10.2 Validity

The validity of the research can be defined as the best available approximation to the truth of a given proposition, inference, or conclusion (Trochim, 2020). Validity has been subdivided into four types: Conclusion Validity, Internal Validity, Construct Validity, and External Validity (Trochim, 2020). This section outlines the importance of each of these aspects of validity and the steps taken to address the validity issues in this study.

Conclusion Validity is the degree to which the conclusions made about a relationship are reasonable, credible and believable. The conclusion of a study is considered valid if the results are likely to be replicated if the study was conducted by another researcher (Trochim, 2020). Conclusion validity is only concerned with whether there is a relationship, or there is no relationship. Threats to conclusion validity include making two kinds of errors:

1. Conclude that no relationship exists when in fact there is one
2. Conclude that a relationship exists when in fact there is none

These errors may arise if the researcher is not alert to the assumptions made during the analysis. For example, if the findings from a literature review are not repeatable under the same conditions, research bias could have unduly affected the initial results. To address conclusion validity, this study assures the reliability of the measure by using a structured literature review protocol which was piloted and reviewed by other researchers. Furthermore, a standard approach based on the strategy identified by Catherine Dawson (2002, p.69) was used to design the questionnaires for conducting the expert review to evaluate the usability and efficacy of the WBANSecRM framework. The questionnaire was piloted to check whether all relevant information was gathered from the expert review to assure reliability.

Internal Validity is concerned about whether the results reported are, in reality being triggered by researcher interference rather than any other conflicting factor (Braun and Clarke, 2013). This study employed several methods to limit potential threats to internal validity. Firstly, the organisations selected the period over which the WBANSecRM framework was to be implemented. During the implementation of the WBANSecRM framework, no other changes were made to the development process, which helped assure that any effects were due to using the WBANSecRM framework. Furthermore, data triangulation and method triangulation were employed to strengthen the internal validity. Data triangulation uses various data sources, including organisational interviews, and analysing academic research papers, international standards and guidelines related to assuring security and privacy for medical devices. The method triangulation was achieved using multiple experts from academia and industry and an industrial pilot in a WBAN based application development organisation.

Construct Validity focuses on whether theoretical constructs are interpreted and measured correctly or refers to the extent to which a study investigates what it claims to investigate (Gibbert and Ruigrok, 2010). In a research project, to assure a high level of construct validity, the parameters studied must be relevant to the research question (Wright et al. 2010). This study employed expert review of the WBANSecRM framework followed by discussions with supervisors about these comments before reaching an agreement for changes to minimise the threats to the construct validity.

External Validity addresses the degree to which the findings of a research study can be generalised in other contexts beyond the context in which it was initially performed. A study is said to be externally valid if *"the conclusions hold throughout the study domain"* (Wright et al. 2010). This study used the basic architecture of the WBAN application, which consists of a sensor device, mobile app and backend application, and recommendations from AAMI TIR 57 and ISO 80001-2-2 to develop the WBANSecRM framework. Furthermore, this framework also consists of possible threats and vulnerabilities with respective countermeasures that can be tailored for a new WBAN based application in different settings. Additionally, the WBANSecRM framework outlines the process to identify the threats and vulnerabilities if any new asset is added in a new environmental context. Finally, this framework was validated by conducting expert reviews with experts from both academia and industry.

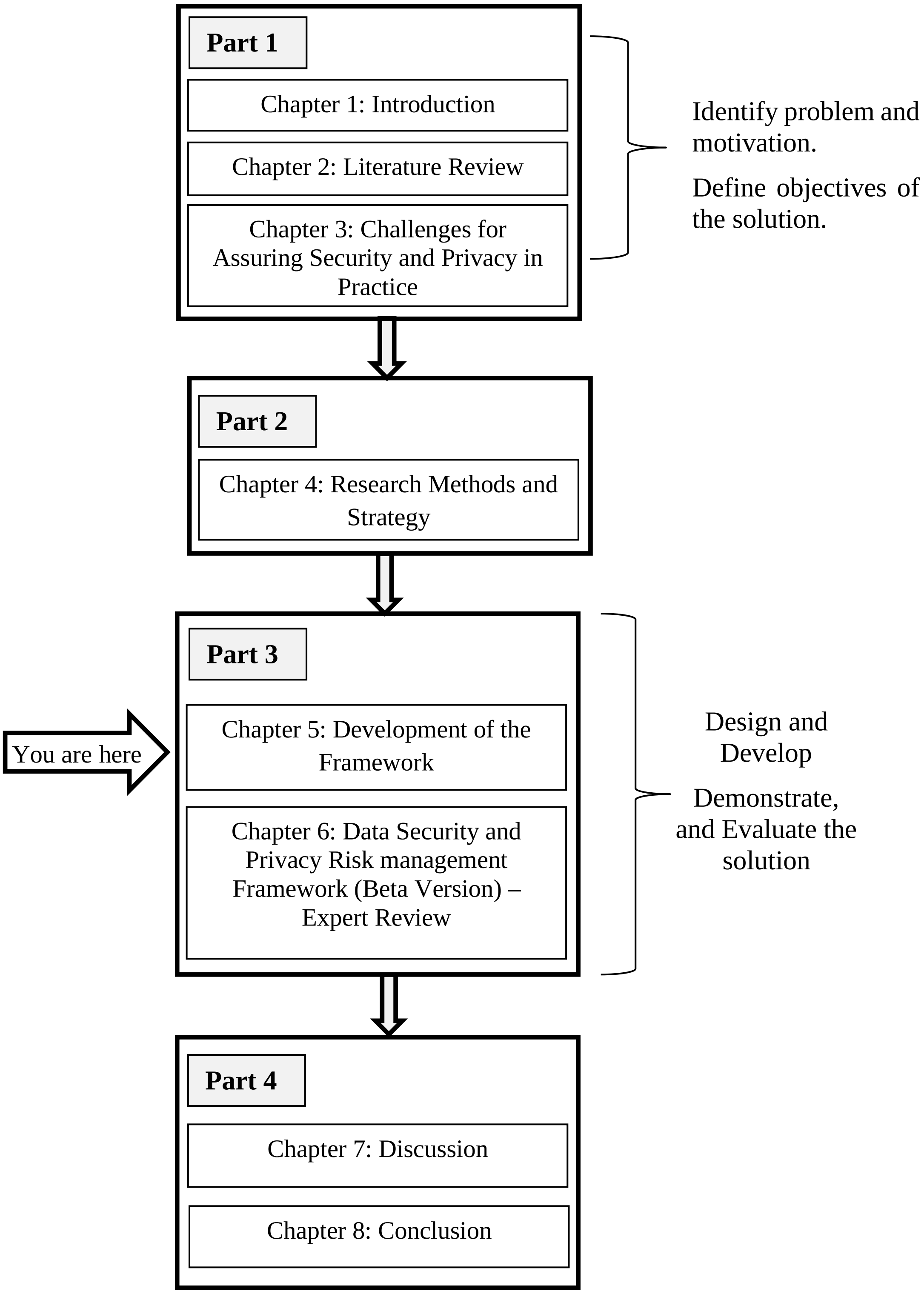
4.11 Summary

This study's research perspective is pragmatism as it involves field-based components (interviews and organisation trials of models), which involves qualitative and quantitative techniques. This mixed-method research is underpinned by pragmatism. Initially, an inductive approach is taken to gather information and the theory developed (WBANSecRM framework to assure security and privacy). A deductive approach was taken to test the theory based initial framework which was trialled in a testbed organisation. A mixed method approach is used in this study to collect qualitative data through interviews within organisations and quantitative data through the expert review. The research strategy chosen for this study is Action Design Research for the following reasons:

- The researcher identified and formulated the problem by executing the literature review and interviews
- Given the nature of this research and the nature of threats and vulnerabilities in WBAN applications, artefact development required close collaboration with organisations
- ADR allowed the researcher and practitioner to collaborate using a rigorous iterative cycle during the early stage of the development of the WBANSecRM framework
- The researcher produced an artefact in the form of a framework that validated in the context in which it will be used
- The outcome of this study produced a generalised version of the artefact

The final section of this chapter considers research quality and outlines the steps taken in this study to mitigate threats to reliability and validity. To help assure reliability, the WBANSecRM framework produced in this study was developed based on the guidelines provided by AAMI TIR 57. Additionally, this study documented the comments received during the expert review phase and how those comments were incorporated in the next version of the WBANSecRM framework. To address conclusion validity, this study assures the reliability of the measure by using a structured literature review which was piloted and reviewed by other researchers. Additionally, a standard approach was used to design the questionnaires for conducting the expert review to evaluate the usability and efficacy of the WBANSecRM framework. The protocol was piloted to check whether all relevant information was gathered from the expert review to assure reliability. Furthermore, a protocol was also used to analyse the expert review comments and to address the respective experts' comments. Data triangulation and method triangulation were employed to strengthen the internal validity. To limit threats to construct validity, an expert review of the WBANSecRM framework was conducted and each comment from the experts was discussed with supervisors before reaching an agreement for changes.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
You are here
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

5 Development of the WBANSecRM Framework

This chapter details the development of the Data Security and Privacy Risk Management Framework (WBANSecRM framework). As discussed in Chapter 3, section 4.8, Action Design Research is the research methodology adopted in this thesis. Stage 2 and stage 3 of ADR define the objectives of a solution to an identified problem. The two main research objectives of this study were identified in Chapter 1. The first objective (RO 1) is the design and development of a framework which will assist developers and organisations to assure security and privacy of WBAN based healthcare applications. Figure 5-1 illustrates the approach taken to develop the WBANSecRM framework.

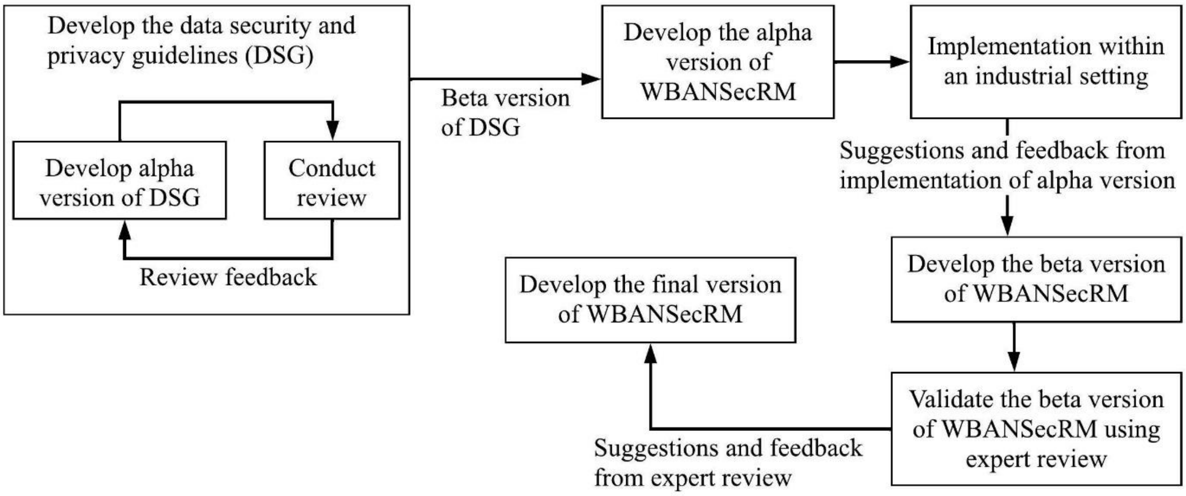

Develop the data security and privacy guidelines (DSG)
Develop alpha version of DSG
Conduct review
Review feedback
Beta version of DSG
Develop the alpha version of WBANSecRM
Implementation within an industrial setting
Suggestions and feedback from implementation of alpha version
Develop the beta version of WBANSecRM
Validate the beta version of WBANSecRM using expert review
Suggestions and feedback from expert review
Develop the final version of WBANSecRM

Figure 5-1: Development approach of the WBANSecRM framework

Following the ADR methodology, the initial development of the WBANSecRM framework was based on a literature review and an interview conducted within Company A. The literature review identified a total of twenty-two security and privacy requirements. Furthermore, an interview with Company A indicated that developers and organisations face challenges implementing countermeasures due to limited implementation details in the existing standards. Implementation guidelines for the controls were developed, named *"Data Security and Privacy Guidelines (DSG)"* in this thesis. The methodology used for developing the implementation details is outlined in section 5.1. The data security and privacy guidelines were reviewed with a team from Company A which consisted of the CTO, Tech Lead and a senior developer. This same group participated in the interview to identify the challenges of implementing safeguards for assuring security and privacy. Several iterations of this review resulted in the beta version of the DSG. For each iteration the DSG were updated based on feedback. An alpha version of the WBANSecRM framework was created, which was subsequently refined based on the suggestions and feedback received from the implementation within an industrial setting. The feedback received after the alpha version's industrial trial resulted in the beta version of the WBANSecRM framework.

Section 5.2 discusses the structure of the alpha version, while section 5.3 outlines the implementation process of the alpha version. Section 5.4 outline the implementation of the alpha version within an industrial setting. Section 5.5 presents the approach taken to develop the beta version, while section 5.6 details the structure of the beta version. Finally, section 5.7 provides a summary of the chapter. The next chapter in this study details the approach taken to validate the beta version of the WBANSecRM. The next chapter also reports the findings and modifications made as a result of performing the expert review.

5.1 Development of the Data Security and Privacy Guidelines

This section details the development of the data security and privacy guidelines for the security and privacy requirements identified during the literature review. As discussed in Section 2.8.2, there are several popular standards for assuring data security and privacy. NIST and the International Organization of Standardization (ISO) are leading standards providers. ISO/IEC 80001-2-2 is a technical report which is specifically designed for developing healthcare applications. This technical report presents an informative set of common, high-level security and privacy related capabilities useful for understanding the user needs, the type of controls to be considered and the risks that lead to the controls. Furthermore, this technical report is also recommended by several regulatory bodies such as the FDA and HIPAA. Therefore, in this research, the ISO/IEC 80001-2-2 standard was selected as the primary standard for developing data security and privacy guidelines for WBAN based healthcare applications. Three steps, illustrated in Figure 5-2, were followed to identify appropriate security and privacy controls and develop the implementation guidelines.

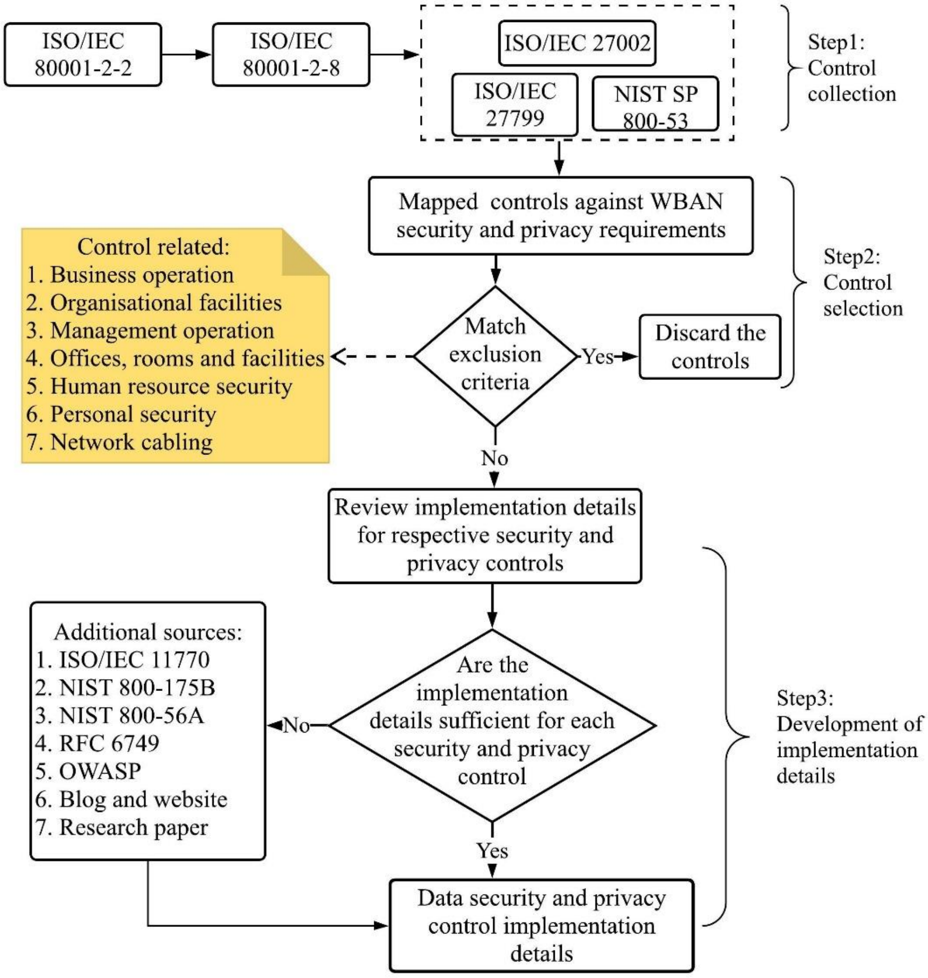

ISO/IEC 80001-2-2
ISO/IEC 80001-2-8
ISO/IEC 27002
ISO/IEC 27799
NIST SP 800-53
Step1: Control collection
Mapped controls against WBAN security and privacy requirements
Control related:
1. Business operation
2. Organisational facilities
3. Management operation
4. Offices, rooms and facilities
5. Human resource security
6. Personal security
7. Network cabling
Match exclusion criteria
Yes
Discard the controls
Step2: Control selection
No
Review implementation details for respective security and privacy controls
Additional sources:
1. ISO/IEC 11770
2. NIST 800-175B
3. NIST 800-56A
4. RFC 6749
5. OWASP
6. Blog and website
7. Research paper
No
Are the implementation details sufficient for each security and privacy control
Yes
Data security and privacy control implementation details
Step3: Development of implementation details

Figure 5-2: Data security and privacy control implementation details development process

5.1.1 Control Collection

The ISO/IEC 80001-2-2 technical report provides 19 security and privacy capabilities with high-level details for Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs). These capabilities include categories of technical, administrative or organisational controls to manage risks to confidentiality, integrity, availability and privacy of data and systems. The ISO/IEC 80001-2-8 (ISO/IEC 80001-2-8, 2016) technical report provides controls to establish the capabilities identified in ISO/IEC 80001-2-2. ISO/IEC 80001-2-8 also provides controls from other standards such as NIST 800-53 (NIST, 2013); ISO

27002 (ISO/IEC 27002, 2017); and ISO 27799 (ISO 27799:2008, 2016). These controls will help HDOs and MDMs to implement each capability identified in ISO/IEC 80001-2-2. In this step, all the controls for the respective capabilities were collected for further analysis. Appropriate controls were selected using exclusion criteria and a review process which is described in the next step.

5.1.2 Control Selection

Each control was mapped to the WBAN security and privacy requirements identified through the literature review presented in Section 2.6.2. The appropriate controls were then selected by excluding controls that related to:

- Business operation
- Organisational facilities
- Management operation
- Offices, rooms and facilities
- Human resource security
- Personal security
- Network cabling

The above controls were excluded because the review of the controls indicated that these controls were not required for assuring security and privacy of the application. For example, the *"Network cabling"* control outlines the policy that needs to be considered during the setup of an office network. Furthermore, the *"Human resource security"* control outlines the human resources related policy for managing existing resources and for onboarding new resources.

5.1.3 Development of Security and Privacy Control Implementation Details

As stated earlier, ISO/IEC 80001-2-8 refers to other standards such as NIST 800-53, ISO 27002 or ISO 27799 for implementation guidelines. Each control's implementation details were extracted from the respective standards for review. The review team was composed of the researcher, a tech lead and a senior developer from Company A. During the review process, each control's implementation details were checked for whether it had enough detail for developers to implement. If the implementation details were not adequate, then further details were selected from other sources. Other sources included standards or technical reports such as OWASP guidelines, blogs, websites and scientific research papers. For example, the ISO/IEC 80001-2-8 standard proposes a key management process as a risk control to generate, distribute and revoke a cryptographic key. For the key management process, the standard refers to section 10.1.2 of ISO 27002 for further details. Section 10.1.2 of ISO 27002 provides very high level and generic details about a key management process and does not provide any information about how the key will be generated and how it will be transferred from the mobile application to the sensor device. ISO 27002 again refers to another standard ISO/IEC 11770 (ISO 11770, 2018) for further details about key management; however, ISO/IEC 11770 only outlines details about key generation and not about key transfer. The developers needed to review three different standards in the above example to find implementation details for key management. A goal of this framework is to provide implementation details for each security and privacy control presented in Appendix C. As an example, implementation details for key management, which a developer can quickly adopt, are outlined below:

- A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented throughout their whole lifecycle (NIST 800-53 SC-12, ISO 27002 10.1.2)
- Create keys with appropriate key size and block size. Do not use a laptop or self-designed application to generate the key. Only generate the key using an application or service provider which supports hardware security modules (HSMs) (ISO/IEC 11770)
- Do not use any self-designed or weak cryptographic algorithms. Select only those which are lightweight and recognised by different standards. For example, AES, DES

and TDEA are currently recognised by the Federal Government standard body for symmetric techniques (NIST 800-175B)

- Consider the proper key size during cryptographic algorithms. For AES 128, 168 or 256-bits key size can be used (NIST 800-175B)
- Generated keys need to be distributed securely by assuring confidentiality and integrity (ISO/IEC 11770)
- Use key wrapping techniques to exchange keys between mobile applications and devices. Diffie-Hellman provides the capability for two parties to agree upon a shared secret for exchanging keys over a public channel (NIST 800-56A)
- If any user or device is identified as compromised, the respective key of the user or device needs to be removed from the application and key management server. After the revocation of a compromised key, a new key needs to be generated and distributed using the above steps (ISO/IEC 11770)
- Log each activity related to key management and use this data to perform auditing (ISO 27002 10.1.2)

5.2 Structure of the Alpha Version of the WBANSecRM Framework

The alpha version of the data security and privacy framework consists of the following three stages:

1) Identification of possible threats and vulnerabilities
2) Implementation of controls to protect the application against those threats and vulnerabilities
3) Evaluation of the efficacy of the controls

Identification of threats: To identify the threats and vulnerabilities, a structured process is required to examine how vulnerable an application is and which types of attack can be launched to compromise the application. Threat modelling and attack trees are widely recognised processes for identifying the possible threats and vulnerabilities to an application, and are considered a significant step in assuring security and privacy. Threat modelling helps assure system security by understanding an adversary's goals and targets in attacking a system based on its important assets (Bedi *et al.*, 2013). Threat modelling also helps to specify the security and privacy requirements throughout the development of an application (Oladimeji, Supakkul and Chung, 2006). Threat modelling activities will start with defining the scope and data flow of the application. Several tools and methods are available to conduct threat modelling, such as STRIDE, LINDDUN, the Process for Attack Simulation & Threat Analysis (PASTA), and Trike.

Control implementation: Once the threat modelling process is complete, the next task is to analyse the threat modelling report to identify the appropriate controls to mitigate the threat or vulnerability. During the review process, each threat description, threat category and data flow interaction needs to be considered. In some cases, if a threat does not contain enough detail, then the threat category will be used to select a control as a countermeasure. Upon completing the security and privacy control selection process, the next task was to implement the controls. Implementation details for each control are outlined in Appendix B. The examples below illustrate the implementation details for the ‘Weak authentication scheme’ vulnerability.

Vulnerability name: Weak authentication scheme

Control: Authentication

Implementation details:

- Force users to have a strong password.
- Do not display or transmit the password in clear text. Validate the email address and password through an input validation technique. Validate email address by sending an email verification link.
- Lock user accounts after a certain number of failed login attempts during a time-period.

- Maintain a list of commonly used, expected, or compromised passwords and update the list when passwords are compromised directly or indirectly.

Evaluation of control efficacy: To evaluate the efficacy of the controls, the organisation needs to employ security testing techniques such as vulnerability scans and/or penetration testing. This security testing will help the organisation to identify to what degree the application will assure the security and privacy of the PHR data. An organisation can conduct vulnerability scans and/or penetration testing by forming a team of people who have technical expertise in conducting vulnerability scans and/or penetration testing. Additionally, an organisation can also on-board external resources to conduct vulnerability scans and/or penetration testing, for example, security consultants.

5.3 Implementation Process of the Alpha Version

Having presented the overall structure of the alpha version of the data security and privacy framework, this section describes the process used for the industrial implementation of the alpha version of the WBANSecRM framework. Figure 5-3 illustrates the implementation process of the alpha version of the data security and privacy framework.

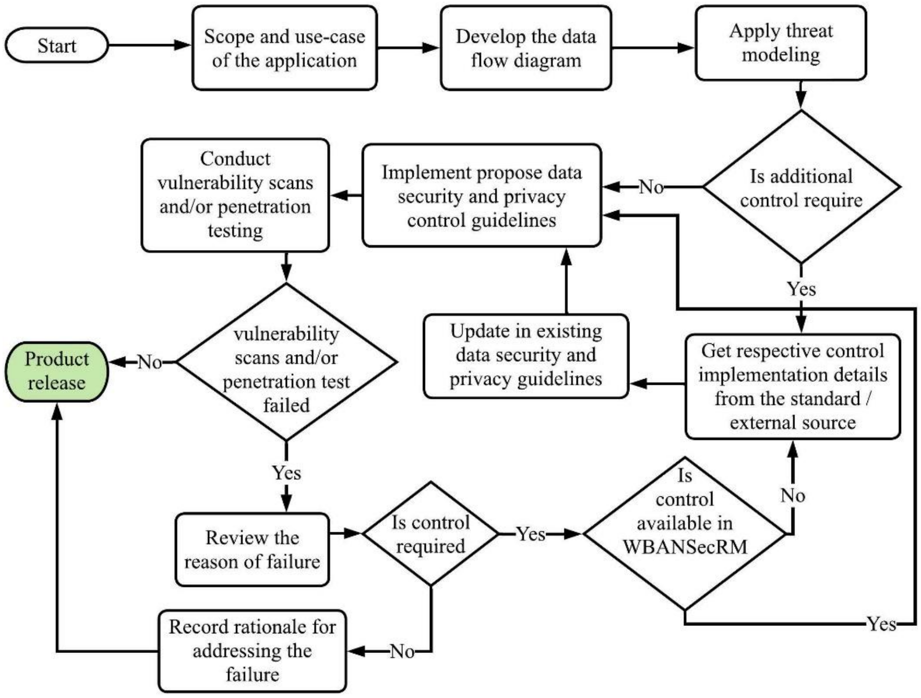

Start
Scope and use-case of the application
Develop the data flow diagram
Apply threat modeling
Is additional control require
No
Yes
Implement propose data security and privacy control guidelines
Conduct vulnerability scans and/or penetration testing
vulnerability scans and/or penetration test failed
No
Product release
Yes
Update in existing data security and privacy guidelines
Get respective control implementation details from the standard / external source
Review the reason of failure
Is control required
Yes
Is control available in WBANSecRM
No
Yes
Record rationale for addressing the failure
No

Figure 5-3: Implementation process of the data security and privacy framework (alpha version)

Implementing the data security and privacy framework commences by defining the scope and the WBAN application use-cases. The developer then needs to convert the proposed use-cases into a data flow diagram used as input for the threat identification process. As discussed in the previous section (Section 5.2), a threat modelling technique is used as part of the threat identification process. The threat modelling will produce a list of threats and vulnerabilities for the application. The developer needs to check in Table Appendix E-1 for the respective control for the threats and vulnerabilities. If all the threats and vulnerabilities are available in Table Appendix E-1 then the developer needs to implement the individual security and privacy controls to mitigate the identified threats and vulnerabilities. Furthermore, suppose any identified threats and vulnerabilities are not available in Table Appendix E-1. In that case, the developer needs to find the respective control's implementation details from the standards or external sources and update the existing security and privacy guidelines. Finally, to evaluate the efficacy of the control, vulnerability scans and/or penetration testing needs to be conducted upon completion of the control implementation. Upon completion of vulnerability scans and/or penetration testing, if there is a failure the development team needs to review the reason for failure. If no control is required to address the failure, the team must record the rationale for addressing the failure. If additional controls are required, the developer needs to find the respective security and privacy controls from Table Appendix E-1. If the control is not available in the Table Appendix E-1 then the developer needs to find a suitable control from the external sources and implement the control. Once the control is implemented, they need to re-run the vulnerability scans and/or penetration testing to validate that the threat is mitigated.

Implementation of the Alpha Version

5.4 Implementation of the Alpha Version Within an Industrial Setting

The purpose of this section is to demonstrate the implementation details for alpha version of the framework. This section also outline the results of threat modelling, which was conducted on Company A’s WBAN application, along with the security and privacy controls which were implemented as a result of vulnerabilities identified through the threat modelling. Finally, the results of a penetration test are presented. The penetration test was conducted in order to verify to what degree the controls assure security and privacy of the WBAN fitness tracking application.

5.4.1 Scope and Application Use-Case

The *FitnessX* app is the first consumer product for Company A following on from the success of the core product for professional sports teams. The product uses a phys-ical activity monitor, known as a pod, which uses GPS and a series of sensors to track an athlete’s activity during training and gameplay, and relay this information to the app running on either iOS or Android over Bluetooth. In the app, users can sign up for an account and pair their device, before tracking sessions and syncing this data to the cloud. Sessions generate statistics and analysis which can be used by the individual to track their performance and they can choose to share some of their data in a global leader-board. They can also create mini private or group leagues to use the same lead-er-board functionality among a closed group of individuals.

5.4.2 Develop Data Flow Diagram

A data flow diagram (DFD) is used to provide an overview of the application and graphically represent the flow of the data through an information system or application. A DFD can also provide insight about input and output of data, how data will flow and where it will be stored in an application. There are several levels of DFDs that can be drawn for an application. These are categorised based on the level of complexity. Increasing the level of a DFD increases the complexity. Level ‘0’ and Level ‘1’ are widely used levels of DFD.

5.4.3 Apply Threat Modelling

STRIDE is a widely recognized threat modelling technique for web-based applications. It was developed by Microsoft, which also provide an open-source tool named the Microsoft Threat

Modelling Tool (TMT). This tool includes a graphical interface to conduct threat modelling. By using the graphical interface, a user can easily design the data flow diagram, configure necessary parameters and track the threat with respective implementation status. Conducting threat modelling using this tool is carried out in three steps:

- Design and configuration.
- Generate threat report.
- Identify the security controls by analysing the report.

The design and configuration step starts by drawing the Data Flow Diagram (DFD). This DFD diagram is enhanced by adding the proper data flows, data stores, processes, interactors, and trust boundaries. Each of the DFD element properties is configured based on the respective element behaviour. For example, device attribute properties are configured by setting “Yes” to GPS, data, store log data, encrypted, write access, removable storage and backup. After that, each of the DFD elements is connected by defining the proper connectivity attribute. The connectivity attribute is set to “Bluetooth” from device to iOS and Android mobile app, and mobile app to REST API is set to “Wi-Fi”. The REST API to Non-Relational database is configured as “wired” as both are deployed in cloud infrastructure. Finally, a trust boundary is configured to enable the trust level between DFD elements for data exchange. Figure 5-4 illustrates the application’s updated DFD.

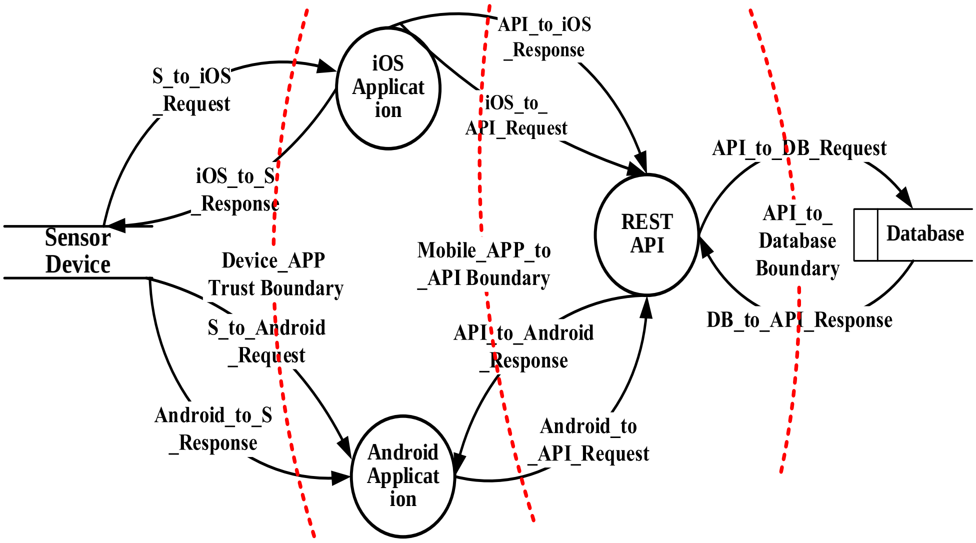


Figure 5-4: FitnessX DFD diagram

One of the key features of the Microsoft TMT tool is the ability to generate a threat report based on the DFD and element attributes. The threat report consists of a list of threats, threat categories, data flow directions and respective descriptions. Table 5-1 illustrates some sample threats and vulnerabilities with their respective descriptions.

Table 5-1: Sample vulnerabilities identified using Microsoft TMT tool

Vulnerabilities	Description
The device data store could be corrupted	Data flowing across iOS_to_S_Response may be tampered with by an attacker. This may lead to corruption of device. Ensure the integrity of the data flow to the data store.
Potential weak protections for audit data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs. Ensure access to the log is through channels which control read and write separately.
Potential data repudiation by REST API	REST API claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Weak authentication scheme	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials and a weak credential change management system.
Potential lack of input validation for REST API	Data flowing across Android_to_API_Request may be tampered with by an attacker. This may lead to a denial of service (DoS) attack against REST API or an elevation of privilege attack against REST API or an information disclosure by REST API.

The description of each threat will help to identify the appropriate security con-trols. After exporting the threat report from the TMT tool, each threat needs to be re-viewed to identify appropriate controls. During the review process, each threat de-scription, threat type and data flow interaction needs to be considered. In some cases, if a threat does not contain enough description of the threat, then the threat category will be used to select a control as a countermeasure. Table 5-2 outlines a snapshot of the list of controls for mitigating the vulnerabilities.

Table 5-2: Mapping of the control for respective vulnerabilities

Vulnerabilities	Control
Weak authentication scheme Authentication Weak credential transit	Authentication, Encryption
Potential data repudiation by Android and/or iOS application	Auditing, Non-repudiation
Potential process crash or stop for REST API due to the DOS attack	Access control, Intrusion detection, Auditing
Lack of data input validation	Data integrity, Input validation
Lack of encryption on transmitted data	Encryption, Communication security
Lack of encryption on private/sensitive data at rest	Encryption
Lack of physical tamper detection and response	Physical protection
Weak remote access controls	Access control
Lack of system hardening	Physical protection, Client platform security

5.4.4 Implementation of the Controls

Upon completion of the security control selection process, the next task was to implement the controls. The developer needed to follow the implementation details outlined in Appendix C for each control. The examples below illustrate the implementation details for one vulnerability from Table 5-2.

Vulnerability name: Weak authentication scheme

Security control: Authentication

Implementation details:

- Force users to have a strong password.

- Do not display or transmit the password in clear text. Validate the email ad-dress and password through an input validation technique. Validate email address by sending an email verification link.
- Lock user accounts after a certain number of failed logins attempts during a time-period.
- Maintain a list of commonly used, expected, or compromised passwords and update the list when passwords are compromised directly or indirectly.

5.4.5 Evaluate the Effectiveness of the Controls

The goal of this stage is to evaluate the effectiveness of the controls implemented to mitigate the threats and vulnerabilities. To carry out this evaluation, a penetration test was conducted with the help of a third-party penetration service provider. The goal of this stage is to evaluate the effectiveness of the controls implemented to mitigate the threats and vulnerabilities. To carry out this evaluation, a penetration test was conducted with the help of a third-party penetration service provider.

5.4.5.1 Scope of the Testing

The scope of the testing consists of what networks, applications, databases, accounts, people, physical security controls and assets will be attacked during the testing. So, the sensor device, mobile application, database, and respective communication medium was set as scope for the testing. Furthermore, a combination of manual and automated tools was used to exploit the system.

5.4.5.2 Testing Tools

As discussed in the previous section penetration testing can be conducted using a combination of manual and automated tools. Table Appendix D- 9 in Appendix D illustrates some of the automated tools used during penetration testing.

5.4.5.3 Penetration Test Result

The penetration tests identified two different types of vulnerabilities. Along with the test result, the penetration service provider also included recommendations on how to mitigate the vulnerabilities. Below is the list of vulnerabilities, along with mitigation recommendations which were identified during the penetration testing:

- Potential denial of service points: During testing, there were four potential DoS points found. These are requests that timeout within 10s due to malformed data inside the payload. These can be run multiple times in multiple threads, driving up the usage and putting stress and strain on the service.

  Recommendation: It was advised that the API endpoints backend code should handle potential malformed data gracefully by input validation. Additionally, a proper HTTP response is needed if an API endpoint failed to process a request, so that the user can retry a request later.

  Action: Added input validation to validate the input data stream. Additionally, an error response code was also added to notify the user that API endpoints were unable to process the malformed input data.

- Security misconfiguration—Stack traces enabled: During testing, it was discovered that stack traces were enabled for some API endpoints.

  Recommendation: It was advised to turn off the stack trace for all endpoints and use a code review process to detect this coding error during development.

  Action: Stack trace was disabled for all the endpoints and the exception was writ-ten into a log file for auditing.

After making the necessary changes in the codebase to address the issues found during the penetration testing, the update was shared with the penetration service provider. A retest of the updated application was conducted, and it was unable to re-produce these vulnerabilities.

5.5 Development of the Beta Version

As discussed in stage 2 of ADR (BIE stage) in section 4.6, the development of the beta version of the WBANSecRM framework was based on the findings from implementing the alpha version. After implementing the alpha version of the WBANSecRM framework in an industrial setting, a follow-up review session was conducted with the CTO and the development team of Company A. The goal of the review session was to gather suggestions and feedback about the usability and efficacy of the WBANSecRM framework. The suggestions and feedback are presented below:

- Identify the threats and vulnerabilities in both the requirement analysis and system architecture phases to produce the security and privacy requirements
- A guideline for the system architecture review would be useful to check whether the relevant security and privacy requirements are taken into consideration
- A risk evaluation process would be helpful to identify the severity level of the threats and vulnerabilities
- A risk treatment process will be useful to identify the risks which require controls to mitigate
- A code review process during the control’s implementation will help to minimise coding errors
- Conduct unit testing during the implementation phase to identify whether the control is implemented correctly.

To address the above suggestions, a review of existing risk management frameworks was conducted to explore the steps and processes to manage security and privacy risk while developing applications. The AAMI TIR 57 is a widely used risk management framework for developing healthcare-based applications. This framework is also recommended by several standards such as ISO 62304 and regulatory bodies such as the FDA. During the development of the beta version, the risk management guidelines provided by AAMI TIR 57 were adopted. Furthermore, security activities in the healthcare application lifecycle guidance provided by IEC 80001-5-1 were also taken into consideration. The beta version of the WBANSecRM framework consists of three different stages:

1) Security and privacy risk assessment
2) Security and privacy risk controls
3) Evaluation of overall residual security and privacy risk acceptability

These stages are similar to AAMI TIR57 but are differentiated as follows:

- AAMI TIR57 does not clearly define how to conduct the security risk assessment at both the requirements analysis and the system architecture phases. This framework provides the steps to perform a security risk assessment at both phases. Additionally, the WBANSecRM framework provides a list of assets, threats and vulnerabilities which are specific to WBAN applications, which can be used as a starting point for conducting security risk analysis
- AAMI TIR57 does not provide any design review guidelines at the system architecture phase. The beta version of the WBANSecRM framework added the design review guidelines recommended by IEC 80001-5-1
- AAMI TIR57 does not include risk treatment to identify unacceptable risks which require controls to mitigate. The beta version of the WBANSecRM framework provides risk treatment steps as part of the security risk assessment
- The beta version of the WBANSecRM framework also consists of a mapping of possible threats and vulnerabilities with respective risk controls along with implementation details for the controls
- The beta version of the WBANSecRM framework consists of secure coding guidelines which developers can use during code review. Furthermore, this framework also presents the steps and tools for conducting automated code review

- The beta version of the WBANSecRM framework provides steps and tools to conduct in-house vulnerability scans and penetration testing

The beta version of the WBANSecRM framework takes initial product requirements as an input but does not perform any validation or verification of the quality of the product requirements. To develop quality product requirements, guidelines provided by ISO/IEC 62304 can be utilised.

5.6 Structure of the WBANSecRM Framework Beta Version

As discussed in the previous section, the beta version of the WBANSecRM framework was developed based on the guidelines provided by AAMI TIR 57. Figure 5-5 illustrates the structure of the beta version of the WBANSecRM framework. The rest of section outlines each stage. A detailed description of the beta version is outlined in Appendix B.

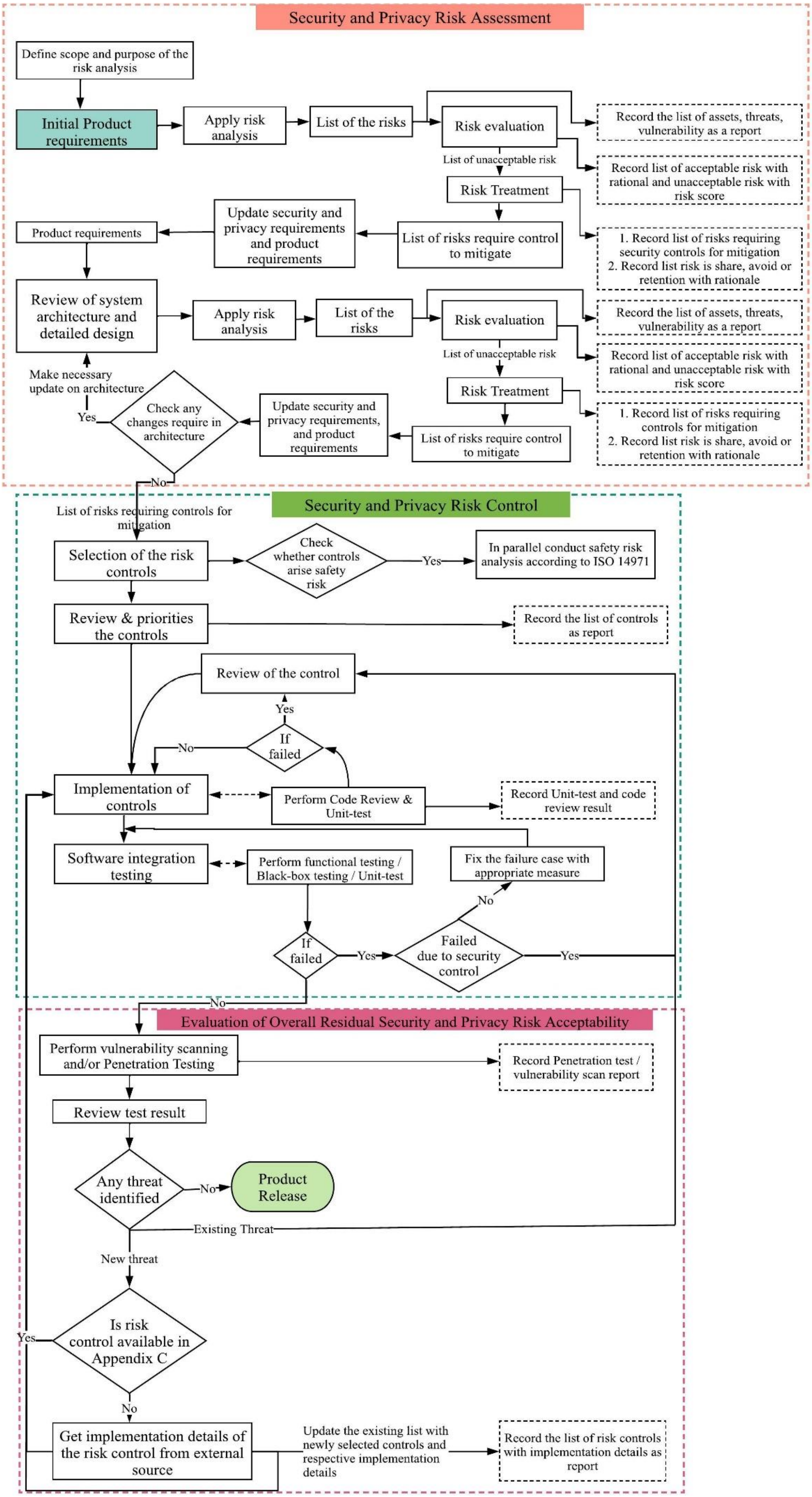

Security and Privacy Risk Assessment
Define scope and purpose of the risk analysis
Initial Product requirements
Apply risk analysis
List of the risks
Risk evaluation
Record the list of assets, threats, vulnerability as a report
List of unacceptable risk
Record list of acceptable risk with rational and unacceptable risk with risk score
Risk Treatment
List of risks require control to mitigate
1. Record list of risks requiring security controls for mitigation
2. Record list risk is share, avoid or retention with rationale
Update security and privacy requirements and product requirements
Product requirements
Review of system architecture and detailed design
Apply risk analysis
List of the risks
Risk evaluation
Record the list of assets, threats, vulnerability as a report
List of unacceptable risk
Record list of acceptable risk with rational and unacceptable risk with risk score
Risk Treatment
1. Record list of risks requiring controls for mitigation
2. Record list risk is share, avoid or retention with rationale
List of risks require control to mitigate
Update security and privacy requirements, and product requirements
Check any changes require in architecture
Yes
Make necessary update on architecture
No
Security and Privacy Risk Control
List of risks requiring controls for mitigation
Selection of the risk controls
Check whether controls arise safety risk
Yes
In parallel conduct safety risk analysis according to ISO 14971
Review & priorities the controls
Record the list of controls as report
Review of the control
Yes
If failed
No
Implementation of controls
Perform Code Review & Unit-test
Record Unit-test and code review result
Software integration testing
Perform functional testing / Black-box testing / Unit-test
Fix the failure case with appropriate measure
No
If failed
Yes
Failed due to security control
Yes
No
Evaluation of Overall Residual Security and Privacy Risk Acceptability
Perform vulnerability scanning and/or Penetration Testing
Record Penetration test / vulnerability scan report
Review test result
Any threat identified
No
Product Release
Existing Threat
New threat
Is risk control available in Appendix C
Yes
No
Get implementation details of the risk control from external source
Update the existing list with newly selected controls and respective implementation details
Record the list of risk controls with implementation details as report

Figure 5-5: Structure of the WBANSecRM framework (Beta version)

5.6.1 Security and Privacy Risk Assessment

The security and privacy risk assessment helps to identify, analyse and evaluate potential security and privacy risks. This assessment will help an organisation to make decisions about which risks require controls for mitigation. To conduct the security and privacy risk assessment, the WBANSecRM framework takes initial product requirements as input and produces lists of assets, threats, and vulnerabilities, followed by a list of security and privacy risks that require controls to mitigate. Figure 5-6 illustrates the steps to perform the security and privacy risk assessment.

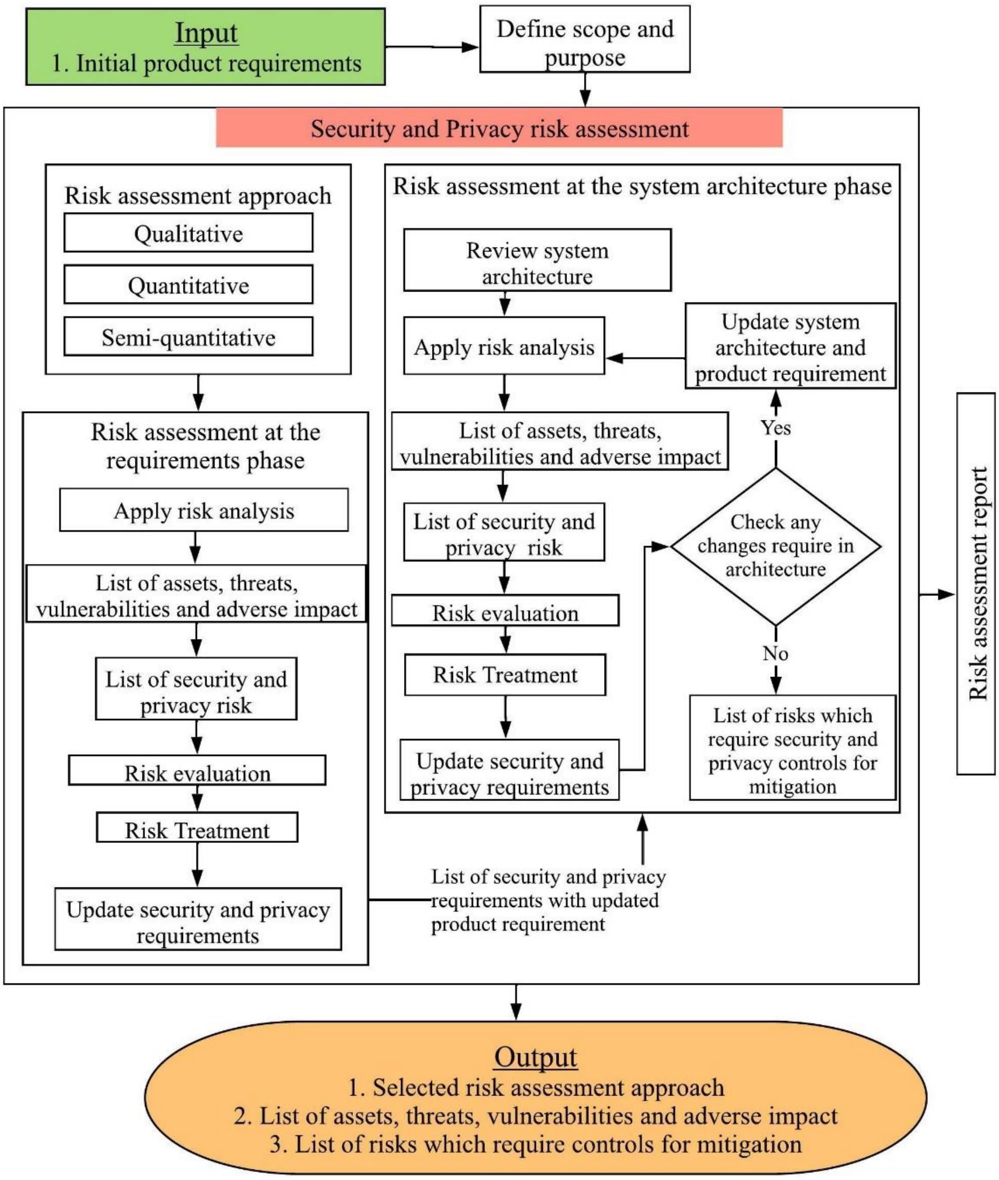

Input
1. Initial product requirements
Define scope and purpose
Security and Privacy risk assessment
Risk assessment approach
Qualitative
Quantitative
Semi-quantitative
Risk assessment at the requirements phase
Apply risk analysis
List of assets, threats, vulnerabilities and adverse impact
List of security and privacy risk
Risk evaluation
Risk Treatment
Update security and privacy requirements
Risk assessment at the system architecture phase
Review system architecture
Apply risk analysis
Update system architecture and product requirement
List of assets, threats, vulnerabilities and adverse impact
Yes
List of security and privacy risk
Check any changes require in architecture
Risk evaluation
No
Risk Treatment
Update security and privacy requirements
List of risks which require security and privacy controls for mitigation
List of security and privacy requirements with updated product requirement
Risk assessment report
Output
1. Selected risk assessment approach
2. List of assets, threats, vulnerabilities and adverse impact
3. List of risks which require controls for mitigation

Figure 5-6: Steps to conduct a security and privacy risk assessment

The security and privacy risk assessment are divided into two key stages;

1) Risk analysis
2) Risk evaluation and treatment

The risk analysis stage aims to identify the assets, threats, vulnerabilities and adverse impacts on an application. To assist with the risk analysis, an organisation may use relevant information obtained from a previously conducted risk analysis of a similar type of product as a starting point. The degree of reusability of data from previous analyses depends on the timeframe of when the last analysis was done on a similar product. The risk evaluation and treatment stage will identify acceptable risks and unacceptable risks, requiring controls to mitigate. The steps for conducting risk assessment at both requirements analysis and system architecture phases is presented in section 4.1 under Appendix B.

5.6.2 Security and Privacy Risk Controls

Security and privacy risk controls are safeguards or countermeasures whose purpose is to mitigate the threats and vulnerabilities to an application. Organisations should form a team to identify, implement and verify the security and privacy risk controls to mitigate unacceptable risks. The team may comprise of the product owner, project manager, technical lead, senior software engineer, developer, QA engineer and QA team. The purpose of this stage is to select, implement and verify security and privacy risk controls. This stage will take a list of unacceptable risks as the input and produce an application with all the necessary security and privacy risk controls implemented and verified. Figure 5-7 presents the steps for selecting and implementing security and privacy risk controls.

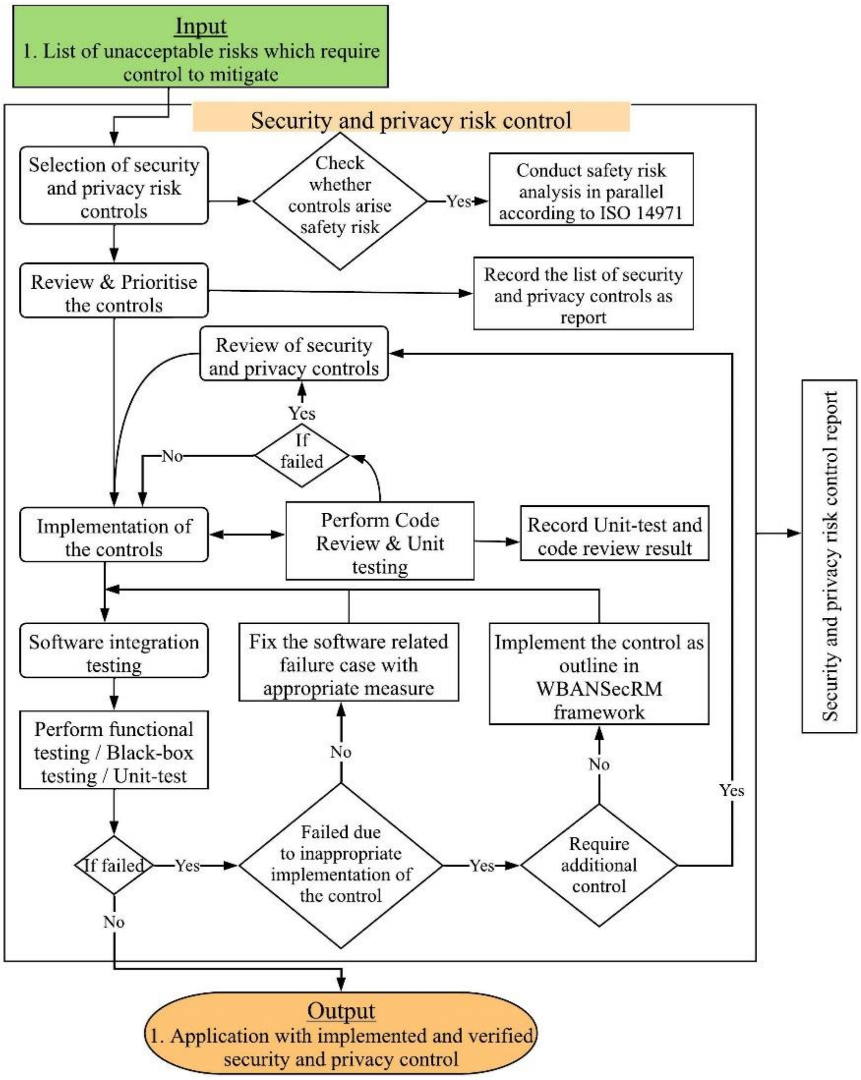

Input
1. List of unacceptable risks which require control to mitigate
Security and privacy risk control
Selection of security and privacy risk controls
Check whether controls arise safety risk
Yes
Conduct safety risk analysis in parallel according to ISO 14971
Review & Prioritise the controls
Record the list of security and privacy controls as report
Review of security and privacy controls
Yes
If failed
No
Implementation of the controls
Perform Code Review & Unit testing
Record Unit-test and code review result
Software integration testing
Fix the software related failure case with appropriate measure
Implement the control as outline in WBANSecRM framework
Perform functional testing / Black-box testing / Unit-test
No
No
Yes
If failed
Yes
Failed due to inappropriate implementation of the control
Yes
Require additional control
No
Security and privacy risk control report
Output
1. Application with implemented and verified security and privacy control

Figure 5-7: Selection and implementation process of security and privacy risk control

In the development phase, the team will implement and verify each of the controls. During the implementation of the security and privacy risk controls, the team should consider secure coding practices. Secure coding practices help reduce the chance of introducing unwanted vulnerabilities during development. The developer will use organisation defined secure coding practices if available; otherwise, the team can follow the secure coding guidelines provided below. Finally, to verify whether controls have been implemented properly, code review and unit testing should be conducted.

Secure coding guidelines:

- Validate input from all data sources
- Compile code using the highest warning level available in the compiler and take necessary action to resolve the warnings
- Use version control to track changes made to the code
- Sanitise the input to SQL statements. Use parameterised SQL statements. Do not use string concatenation or string replacement to build SQL statements.
- Use the latest version of compilers, which often include defences against coding errors; for example, GCC protects code from buffer overflows
- Include proper error/exception handling. Check the return values of every function, especially security-related functions. Also, check for leakage of sensitive information to untrusted users
- Encode HTML input field data. Attackers use malicious input to conduct XSS attacks. Encoding of every user-supplied input can prevent the client's web browser from interpreting these as executable code. Do not store sensitive data in cookies
- Encrypt all confidential data using strong cryptographic techniques. Use a published and strong cryptographic algorithm with a sufficiently long key
- Use code analysis tools to find security issues early

Code review is an effective technique to examine the source code to minimise coding errors and reduce the risk of introducing vulnerabilities during the implementation phase of software development. Secure coding guidelines also need to be considered during the code review process. Code review can be performed manually and/or by using an automated tool. To conduct a manual code review, organisations need to assign an experienced person from the development team. Unit testing is a testing method which helps to test an individual unit or components of an application. The goal of unit testing, from a security perspective, is to verify that each implemented control effectively mitigates its respective security and/or privacy risk. The steps for selection and implementation of security and privacy risk controls is presented in section 4.2 under Appendix B.

Software integration testing is a level of software testing where individual units are combined and tested as a group. Integration tests help to identify whether independently developed units of software work correctly when they are connected to each other. Integration testing can adopt different approaches, such as; Black Box Testing, White Box Testing, and Gray Box Testing methods. During software integration testing, the developer needs to conduct two key tests:

- Security and privacy requirements testing - to validate the security and privacy requirements identified during the security risk assessment steps are implemented properly. This can be achieved by conducting functional, performance and scalability testing
- Threats and vulnerabilities mitigation testing - to validate the effectiveness of the security and privacy controls against the identified threats and vulnerabilities

The following steps should be conducted at the software integration testing stage:

- Perform integration testing by conducting functional testing, unit-test, black-box, white box, and gray box testing. Organisations can use one or a combination of multiple testing approaches to conduct the integration testing based on the QA resource expertise and availability.

  Example integration test cases for WBAN application:

  - Verifying the interface link between the login page and the home page, i.e. when a 'User' enters their credentials and logs in, they should be directed to the homepage
  - Verifying the interface link between the home page and the profile page, i.e. profile page should open up

    - Verifying the interface link between the home page and device page on the mobile app i.e. device page should open up and show connected sensor devices
- If an integration test fails, then check whether it failed due to inappropriate implementation of the security and privacy risk control
    - If no, then take appropriate measures to fix the software related failure case and conduct the software integration test again
    - If yes, then check whether any additional controls are required. If yes, then review the security and privacy controls based on considerations presented in section 4.2.5 of Appendix B. If no, then implement the security and privacy control as outline in Appendix C and conduct the software integration test again

5.6.3 Evaluation of Overall Residual Security and Privacy Risk Acceptability

Upon completion of the risk control implementation and verification stage, the overall residual security and privacy risk needs to be assessed. Evaluating an application’s overall residual security and privacy risk is a complex process as determining how an attacker will exploit the application and the severity level of the exploit is difficult to assess. According to the AAMI TIR 57 standard, an organisation can employ security testing techniques such as vulnerability scans and/or penetration testing to evaluate an application's overall residual security and privacy risk. This stage will take the application with risk controls implemented and verified as input to conduct the vulnerability scans and/or penetration testing. Ideally, the team may comprise the product owner, project manager, technical lead, software architect, senior software engineer and third-party resources (if required) such as penetration testers. Figure 5-8 presents the steps for evaluating the overall residual security and privacy risk of the application.

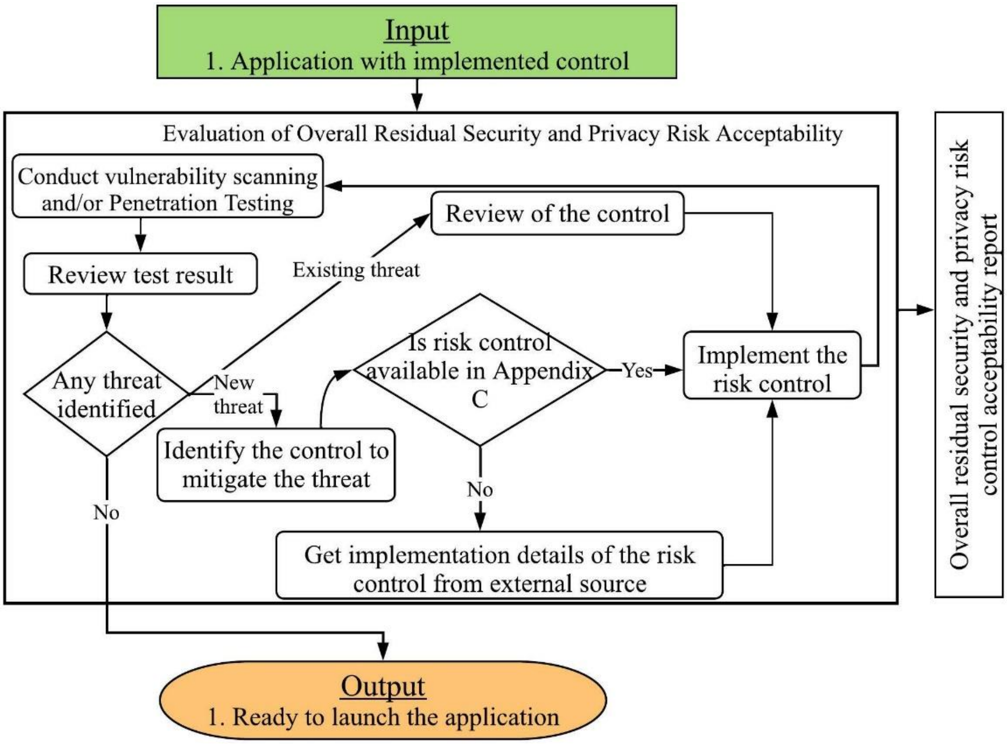

Input
1. Application with implemented control
Evaluation of Overall Residual Security and Privacy Risk Acceptability
Conduct vulnerability scanning and/or Penetration Testing
Review test result
Review of the control
Existing threat
Any threat identified
New threat
Identify the control to mitigate the threat
Is risk control available in Appendix C
Yes
No
Implement the risk control
Get implementation details of the risk control from external source
No
Overall residual security and privacy risk control acceptability report
Output
1. Ready to launch the application

Figure 5-8: Steps for evaluating the overall residual security and privacy risk acceptability

Vulnerability scans and penetration testing are very different from each other, but both serve important functions for evaluating the security and privacy risk controls. A vulnerability scan only discovers known vulnerabilities; it does not attempt to exploit a vulnerability but instead only confirms the possible existence of a vulnerability. An organisation can conduct vulnerability scanning using an automated tool with some manual support. The limitation of vulnerability scanning is that it only scans for known vulnerabilities, provides a list of possible vulnerabilities, and does not confirm whether those vulnerabilities are exploitable or not.

Penetration testing is a security testing approach which identifies exploitable vulnerabilities of a system, or of individual components of a system. Penetration testing helps to replicate the adversary’s actions in carrying out attacks against the application and provides an in-depth analysis of security and privacy-related weaknesses or deficiencies. Penetration testing requires specialised skills, higher budgets and more time than vulnerability scanning. An organisation can conduct penetration testing by forming a team of people within the organisation who have the technical expertise to conduct a penetration test. If an organisation does not possess the required expertise, they can on-board external resources with the required expertise to conduct penetration testing. The detailed steps and tools for evaluating the effectiveness of the risk controls is presented in section 4.3 under Appendix B.

After conducting the vulnerability scanning and/or penetration testing, the results of the testing need to be reviewed. Passing a penetration test/vulnerability scan does not guarantee that the application is invulnerable, however it does mean that the application is at least invulnerable within the scope of the testing. If the vulnerability scanning and/or penetration testing are successful (i.e. do not record a fail), then the organisation can mark the product for launch. If the testing/scanning fails, then the cause of the failure needs to be analysed. To conduct the analysis, the following steps should be followed:

- Check whether the threat is a new threat or existing threat which was identified during the security and privacy risk assessment at the requirements and system architecture phase
- If the threat is an existing threat, then perform a review of the security and privacy risk controls based on the considerations presented below:
    - The security and privacy control was not properly implemented according to the implementation guidelines outlined in Appendix C. In that case the developer needs to implement the security and privacy control again according to the implementation guidelines
    - Appropriate security and privacy risk control was not selected for addressing the threats and/or vulnerabilities
    - The developer did not follow appropriate secure coding practices during implementation of security and privacy risk control

  When the cause of the failure is identified, take appropriate measures to address the failure case and mitigate the identified threat

- If the identified threat is a new threat, then check whether the suggested security and privacy risk control is available in Appendix C
    - If yes, then implement according to implementation details to mitigate the threat and add the selected security and privacy risk control to the existing list
    - If no, then collect implementation details from external sources such as; NIST 800-53, ISO 27005, OWASP, blogs etc. Update the existing implementation details list in Appendix C with the newly identified threat and respective security and privacy risk control with implementation guidelines
- Upon completion of the implementation of the security and privacy risk control, testing/scanning needs to be conducted again to verify that the control successfully mitigates the identified threat
- Document the action taken to address each threat in the overall residual security and privacy risk acceptability report

5.7 Summary

This chapter has presented the development of the WBANSecRM framework. The development of the alpha version of the WBANSecRM framework was based on a literature review and an interview conducted within Company A. The interview with Company A indicated that developers and organisations face challenges implementing countermeasures due to limited implementation details in the existing standards. Implementation guidelines for the controls were developed as part of the alpha version of the WBANSecRM framework. These guidelines are referred to as the “Data Security and Privacy Guidelines (DSG)” and can found in Appendix C.

The development of the DSG consists of three stages: (1) Control collection, (2) Control selection and (3) Development of implementation details. The ISO/IEC 80001-2-2 standard was selected as the primary standard for control collection. After that, each control was mapped to the WBAN security and privacy requirements identified through the literature review. Finally, each control's implementation details were extracted from the respective standards for review. During the review process, each control's implementation details were checked for whether it had enough detail for developers to implement. If the implementation details were not adequate, then further details were selected from other sources. Other sources included standards or technical reports such as OWASP guidelines, blogs, websites and scientific research papers.

The alpha version of the data security and privacy framework consists of the following three stages: (1) Identification of possible threats and vulnerabilities of the application, (2) Implementation of controls to protect the application against those threats and vulnerabilities, and (3) Evaluation of the efficacy of the controls. To identify the threats and vulnerabilities, a threat modelling process was used. Once the threat modelling process was completed, the threat modelling report was analysed to identify the appropriate controls to mitigate the threats and vulnerabilities. During the review process, each threat description, threat category and data flow interaction was taken into consideration. To evaluate the efficacy of the controls, the organisation can employ unit-testing and security testing techniques such as vulnerability scans and/or penetration testing. This security testing will help the organisation to identify to what degree the application will assure the security and privacy of PHR data.

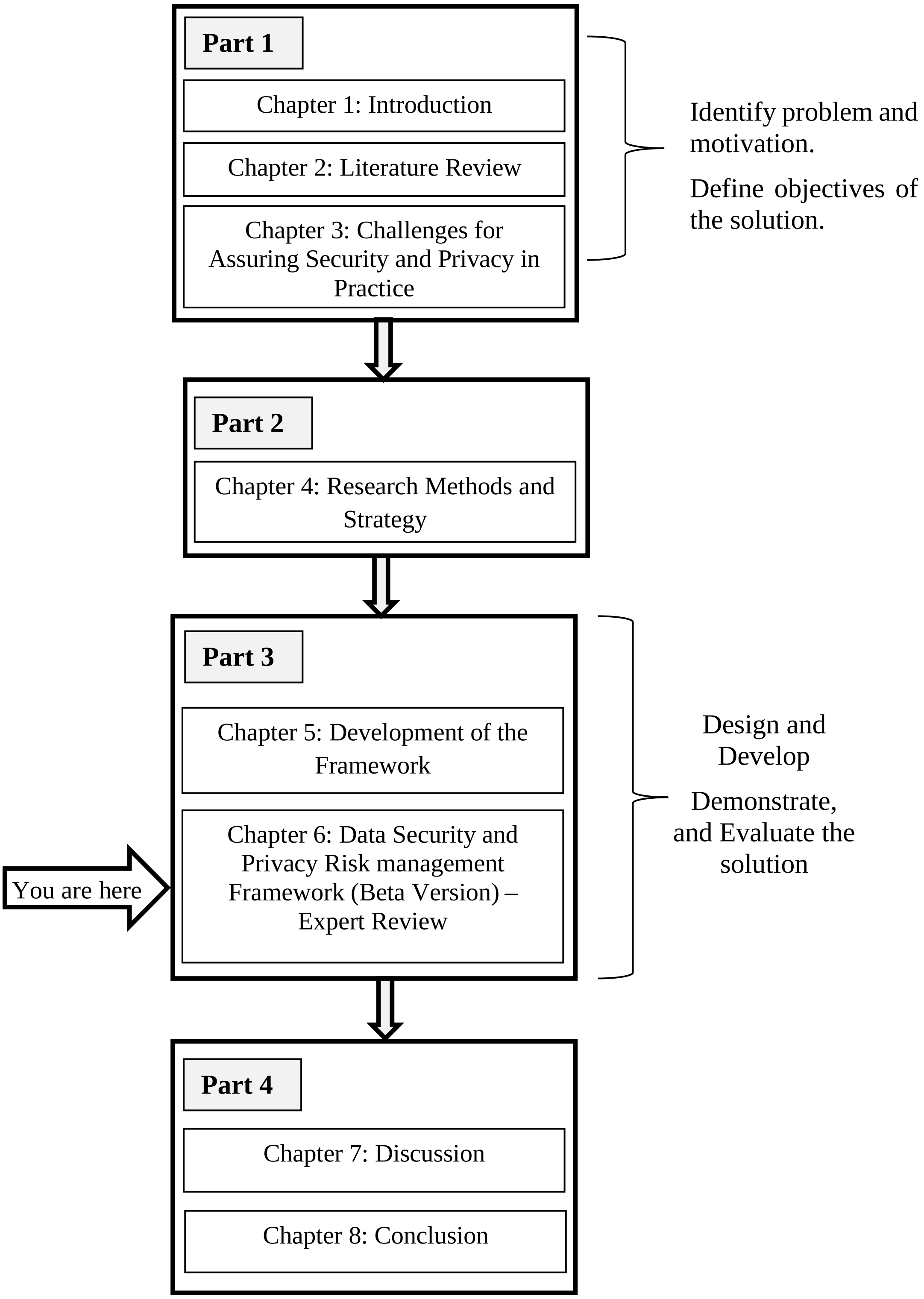
The beta version of the WBANSecRM framework was based on the suggestions and feedback identified from implementing the alpha version within Company A. During the development of the beta version, the risk management guidelines provided by AAMI TIR 57 were adopted. Furthermore, security activities in the healthcare application lifecycle guidance provided by IEC 80001-5-1 were also taken into consideration. The beta version of the WBANSecRM framework consists of three different stages: (1) Security and privacy risk assessment, (2) Security and privacy risk controls and (3) Evaluation of overall residual security and privacy risk acceptability. The beta version of the WBANSecRM framework takes initial product requirements as an input but does not perform any validation or verification of the quality of the product requirements. The security and privacy risk assessment helps to identify, analyse and evaluate potential security risks. This assessment helps an organisation to make decisions about which risks require controls. Security and privacy risk controls are safeguards or countermeasures whose purpose is to mitigate the threats and vulnerabilities. This stage will take a list of unacceptable risks which require controls as the input and produce an application that has all the necessary risk controls implemented and verified. The beta version of the WBANSecRM framework recommends that the organisation can employ security testing techniques such as vulnerability scans and/or penetration testing to assess the overall residual security and privacy risk of an application.

The beta version of the WBANSecRM is differentiated from the alpha version with the following points:

- Developed based on the guidelines provided by AAMI TIR 57, a widely used risk management framework and IEC 80001-5-1 for security activities in the healthcare application lifecycle
- Identify the threats and vulnerabilities in both the requirement analysis and system architecture phases to produce the security and privacy requirements
- Provide guidelines for conducting the system architecture review to check whether the relevant security and privacy requirements are taken into consideration
- A risk treatment process to identify the risks which require controls to mitigate
- A code review process to minimise the coding errors
- Conduct unit testing during the implementation phase to identify whether the control is implemented correctly

The next chapter in this study details the approach taken to validate the beta version of the WBANSecRM framework.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
You are here
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion

6 Data Security and Privacy Risk management Framework (Beta Version) – Expert Review

This chapter details the validation of the beta version of the WBANSecRM framework by expert review. It also reports on the findings and modifications made as a result of performing the expert review. The expert review was performed as part of stage 2 (Building Intervention and Evaluation) of the Action Design Research Methodology outlined in Figure 4-4 of the Research Methodology chapter. The validation by expert review builds on by industry implementation which has been presented in Chapter 5.

6.1 Approach to the Expert Review of the Data Security and Privacy Risk management Framework (Beta Version)

The approach taken to validate the beta version of the WBANSecRM framework by expert review is presented in Figure 6-1. The expert review was completed in five stages. The first stage was to develop the questionnaire, followed by recruiting appropriate experts. The steps to develop the twenty questions in the questionnaire are outlined in section 6.2. The questionnaire is available in Appendix F. The questionnaire and beta version of the WBANSecRM framework were then presented to experts for review. The criteria for selecting the experts, along with their profiles is presented in section 6.3. On return of the completed questionnaire, the comments received from the experts were analysed by the author of this study to ascertain the usability and efficacy of the WBANSecRM framework beta version. The methodology for conducting this analysis is presented in section 6.4. Once this analysis was complete, the comments and changes needed to address the respective comments were reviewed by a focus group. The focus group consisted of the author and two members of the RSRC. The steps taken to analyse the comments are presented in section 6.5. The focus group reviewed the experts' comments and the suggested changes, and through discussion a consensus was reached on which changes should be adopted. Finally, changes to the

WBANSecRM framework beta version were agreed by the focus group. These are presented in section 6.6.

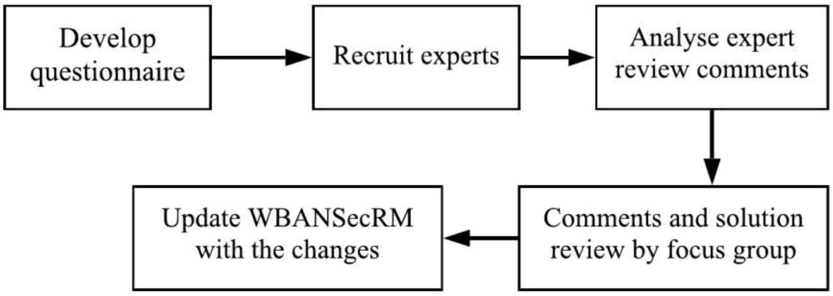

Develop questionnaire
Recruit experts
Analyse expert review comments
Comments and solution review by focus group
Update WBANSecRM with the changes

Figure 6-1: WBANSecRM framework expert review approach

6.2 Develop Questionnaire

The strategy used to develop the questions is based on the strategy identified by Catherine Dawson (2002, p.69). The question development phase contained eight steps illustrated in Figure 6-2. The first step involved considering the purpose of the expert review and what information the researcher sought from the expert review. The purpose of the expert review is to assess the efficacy and usability of the WBANSecRM framework in assuring the security and privacy of WBAN applications.

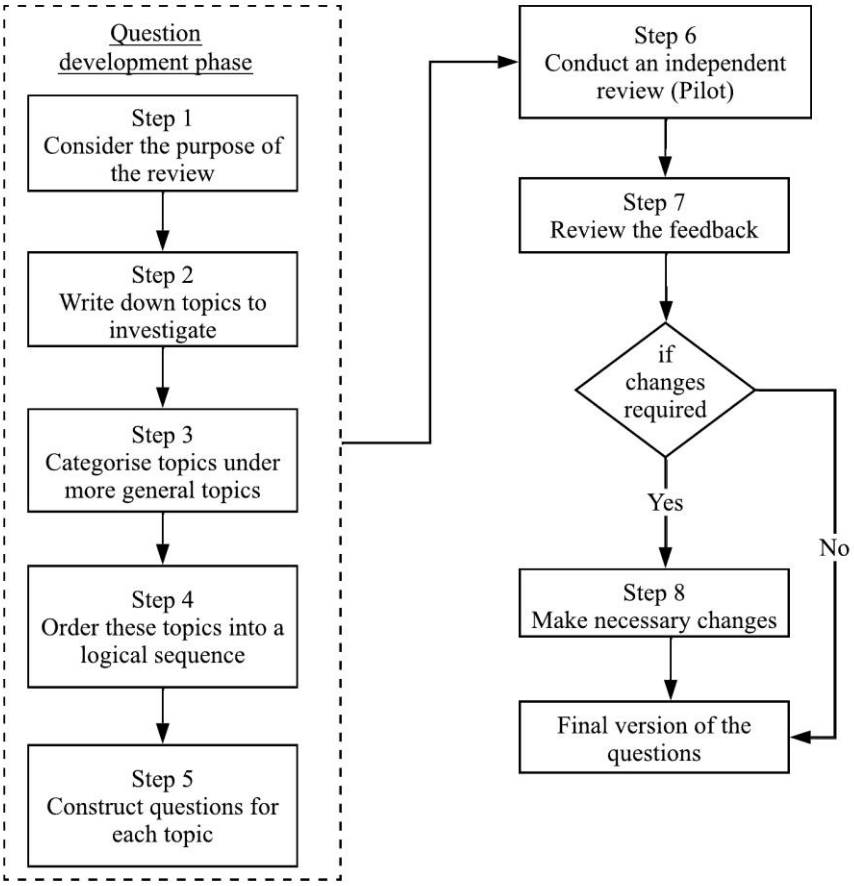

Question development phase
Step 1
Consider the purpose of the review
Step 2
Write down topics to investigate
Step 3
Categorise topics under more general topics
Step 4
Order these topics into a logical sequence
Step 5
Construct questions for each topic
Step 6
Conduct an independent review (Pilot)
Step 7
Review the feedback
if changes required
Yes
No
Step 8
Make necessary changes
Final version of the questions

Figure 6-2: Expert review questionnaire development method

Step 2 of this phase was to identify the topics to be investigated during the expert review. Below is the list of topics that were identified:

1. Each participant's experience in medical device/WBAN based software development/software development with security and privacy
2. Each participant's experience in developing an application (other than medical device/WBAN) with security and privacy
3. Each participant's experiences in legislation, such as HIPPA and GDPR
4. Each participant's experience in the risk management process
5. The suitability of the steps adopted to identify security and privacy risks in the requirements analysis phase
6. Useful tools or sources to identify threats and vulnerabilities
7. The suitability of the steps adopted to identify security and privacy risks based on application system architecture

8. Useful tools or techniques to identify risks using application system architecture
9. The suitability of the steps adopted to identify the controls for respective risks
10. The suitability of the steps adopted to assess security and privacy controls during the implementation phase
11. Security and privacy risk acceptance criteria
12. The suitability of the steps adopted to review the security and privacy controls implementation details
13. Tools and techniques to assess the implementation of each control during the implementation phase
14. The suitability of the steps adopted to evaluate overall security and privacy risk controls
15. Tools and techniques for overall security and privacy risk control evaluation
16. Each participant's feedback and suggestions about the usability and efficacy of the WBANSecRM framework

Step 3 involved taking the topics generated in Step 2 and categorising them under more general topics (henceforth known as categories) as depicted in Table 6-1. This was achieved by merging strongly linked topics. For example, topics 11 and 12 above were merged into a single category named evaluation of security and privacy risks (category 3 below). The third column indicates which topics were merged into each category.

Table 6-1: Topics redefined to categories for developing the questionnaire

Category No.	Category	Step 2 Topic
1	General	1,2,3,4
2	Security and privacy risk analysis	5,6,7,8
3	Evaluation of security and privacy risks	11,12
4	Identification and implementation of security and privacy controls	9,10,13,14
5	Overall evaluation of security and privacy controls	15,16
6	Usability and efficacy	17

Step 4 of the question development phase is to order the categories into a logical sequence, generally moving from the more general to the specific. The resulting sequence from this step is presented in Table 6-1 above. For example, the categories commenced with general questions about the participant followed by more specific questions about the WBANSecRM framework.

Step 5 of the question development phase involved constructing questions around each category. The questions are constructed with a combination of open-ended and closed-ended questions. In general, the questions contained a greater proportion of open-ended questions and were kept short, neutral and to the point. With the combination of closed and open-ended questions, this step produced nineteen questions listed in Appendix F.

Step 6 of the questionnaire development was to have the questionnaire independently reviewed. This review was completed by a member of NetwellCASALA (a DkIT based research centre). The reviewer had extensive experience and expertise in software processes for healthcare applications and developing interview questionnaires. A copy of the questionnaire and a statement outlining the purpose of the review was provided to the reviewer to determine how well the questionnaire fulfilled its purpose and assure that it did not contain ambiguity. In step 7, the reviewer provided the following comments after reviewing the questionnaire:

- To add a little more blank space between questions and question parts or employ some other method of better segregating questions and questions parts. The current formatting is visually dense and makes it easy to accidentally miss individual questions.
- Add a question as a final question of the *"have you any additional comments you would like to make?"* type.

Finally, in step 8 it was agreed to adopt both comments, and so the questionnaire was changed to allow more space between questions and to add a final question as stated above. The final twenty questions are presented in Appendix F.

6.3 Recruiting Experts and Participant Profiles

The expert recruitment process started by setting the selection criteria. The selection criteria used are presented below:

- Having research experience in assuring security and privacy for healthcare applications
- Having expertise in developing WBAN based applications
- Having expertise with risk management processes
- Having knowledge of medical device standards and compliance requirements

Around sixty experts were selected and invited to participate in the review after reviewing their profiles, and publications on LinkedIn, ResearchGate and DBLP. The experts were selected if they met any one of the criteria presented above. Among them, only seven replied and showed interest in participating in the review process. Two experts withdrew from the expert review process due to time constraints. A short biography of each of the five experts is presented below.

Expert 1 has been working as a Senior Engineer in a leading research organisation. In this role, he was active in numerous research and industrial projects as a security expert, security and safety requirements analyst and risk analyst. He is particularly interested in the systematic development of secure software-intensive systems and scalable methods for assessing and guaranteeing IT security and functional reliability. He also worked in industry projects that aimed to develop wearable medical devices (diabetes monitoring); these devices were connected to smartphone apps and deployed in a centralized cloud service.

Expert 2 works as a key expert in the area of research and development in methods for the product security lifecycle for a world-leading health technology company. She has more than 30 years of experience in both academia and industry. As an established expert in security risk management methods, she works on automated security support in development and engineering processes. She is also passionate about combining the current state of the art with an analytical understanding of stakeholder needs to improve practice.

Expert 3 has more than ten years' experience in security and privacy in software engineering. She is also a postdoctoral researcher and member of the *Security: Development processes and Middleware* taskforce in a leading research group. She is one of the main forces behind the development and extension of LINDDUN. This privacy-by-design framework provides systematic support to elicit and mitigate privacy threats in software systems. Furthermore, she is also an active member of the Threat Modelling Manifesto organisation.

Expert 4 works as a research associate in a world-leading research centre and has more than 7 years' experience in assuring safety and security of cyber physical systems. Currently, he is researching model-based dependability assessment and assurance, dynamic risk management, and autonomous systems assurance. In addition, he collaborated on several research projects and supported use case owners with privacy risk analysis using the PRIAM methodology.

Expert 5 has over 15 years' experience and works as a research manager for embedded systems security in a world-leading research centre. He actively researched software security and formal verification and validation of software systems, specifically for embedded systems and low-level operating system components. He is particularly interested in security architectures for safety-critical embedded systems and the Internet of Things, and the concept of sustainability in information and communications technology.

6.4 Methodology for Analysing Expert Review Comments

The expert review comments were received in electronic format via email, where review comments were the combination of closed and open-ended answers to the questionnaire. Due to the nature of the responses, the open-ended answers consisted of text with similar concepts in different text locations. The challenges were then to structure the comments into meaningful and analysable data from which conclusions could be drawn. The five-stage approach used to analyse the reviewer comments is detailed in Figure 6-3. This was developed based on the guidelines presented by Saunders, Lewis and Thornhill, (2009, pp.478) for analysing qualitative data.

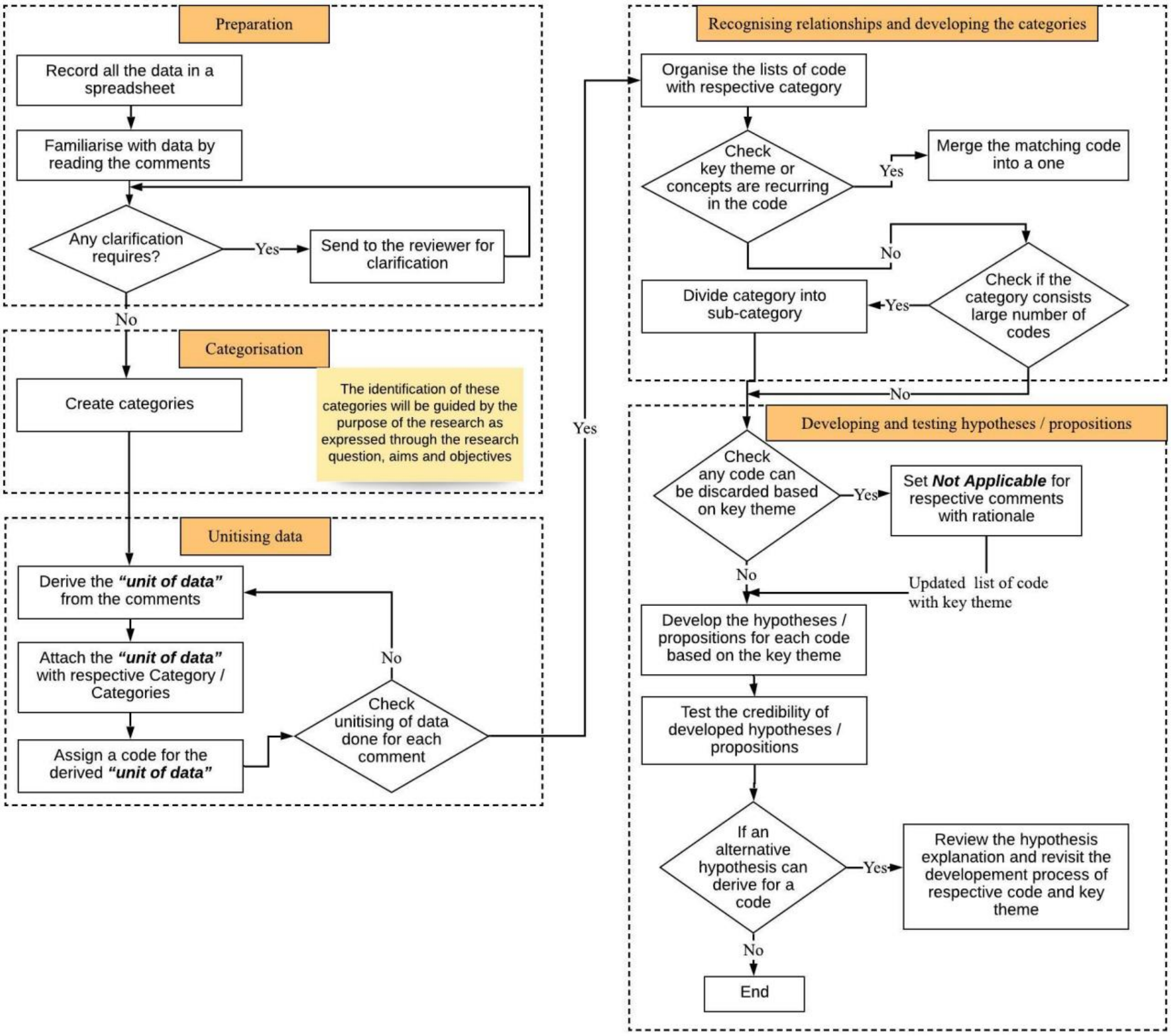

Preparation
Record all the data in a spreadsheet
Familiarise with data by reading the comments
Any clarification requires?
Yes
Send to the reviewer for clarification
No
Categorisation
Create categories
The identification of these categories will be guided by the purpose of the research as expressed through the research question, aims and objectives
Unitising data
Derive the "unit of data" from the comments
Attach the "unit of data" with respective Category / Categories
Assign a code for the derived "unit of data"
Check unitising of data done for each comment
No
Yes
Recognising relationships and developing the categories
Organise the lists of code with respective category
Check key theme or concepts are recurring in the code
Yes
Merge the matching code into a one
No
Check if the category consists large number of codes
Yes
Divide category into sub-category
No
Developing and testing hypotheses / propositions
Check any code can be discarded based on key theme
Yes
Set Not Applicable for respective comments with rationale
Updated list of code with key theme
No
Develop the hypotheses / propositions for each code based on the key theme
Test the credibility of developed hypotheses / propositions
If an alternative hypothesis can derive for a code
Yes
Review the hypothesis explanation and revisit the developement process of respective code and key theme
No
End

Figure 6-3: Methodology for analysing expert review comments

The preparation stage involved recording all the expert comments and the researcher familiarising themselves with the comments. The preparation stage involved the following steps:

3) Record all the comments in a spreadsheet for better visualisation and for ease of analysis, as the experts sent the response electronically in Word format;

4) Read each of the comments and check whether any clarification is required. During this process, two comments were identified that required more context, which was then sent to the respective expert for more detail.

The **categorisation** stage involved creating initial categories based on the expert review objective, research question, and aim of the research, which resulted in the following six categories:

4) **Security and privacy risk analysis** – comments related to the tools, techniques and methods presented in the WBANSecRM framework for identifying security risks, threats and vulnerabilities
5) **Evaluate the security and privacy risks** – relating to the process to determine whether the risks identified in the security risk analysis step are acceptable or not
6) **Security and privacy risk control** – relating to the process for selecting security and privacy controls, along with each control's implementation detail
7) **Overall evaluation of security and privacy risk controls** – approach to evaluate the security and privacy risk level of the application
8) **Usability and efficacy** – whether the WBANSecRM framework is easy to understand and contains sufficient detail
9) **General** – comments about inconsistent terminology, typo errors and explanatory sentences with rationale

Unitising data involves creating units of data from the comments and attaching it to an appropriate category. A unit of data may be a number of words, a transcript line, a sentence, several sentences, a complete paragraph, or some other chunk of textual data that fits the category. Unitising data involved carefully reading the comments several times, each time underlining the content that applied to any sub-category and annotating the underlined content with the sub-category code. This process was repeated until no new text for coding emerged.

As an exemplar, Table 6-2 illustrates the sub-category and unit of data creation for the security and privacy risk control category.

Table 6-2: Illustration of security and privacy risk control category sub-category and unit of data

Category	Unit of Data	Code	Sub-category
Security and privacy risk control	Security and privacy risk control implementation details	Sec_Risk_Con_Imp_Details	Implementation details
	Lack of implementation details	Lack_Imp_Details	
	Split control implementation details in architecture and dev	Split_Con_Imp_Details	
	New security and privacy risk control	New_Sec_Risk_Con	New security and privacy risk control
	New security and privacy control source	New_Sec_Con_Source	
	Security and privacy control selection process	Sec_Con_Selection_Pro	

The next step, **recognising relationships and developing the categories** involved organising the list of codes with their respective categories followed by checking whether the key theme or concepts are recurring in the code. If the concept is recurring, then merge the matching codes. Additionally, check if any categories consist of a large number of codes, then divide the category into a sub-category and attach the appropriate code.

The developing and testing propositions stage involved creating the hypothesis or proposition for each code. Once the proposition was developed for each code, a focus group was set up to review the creditability of the proposition. In this research study, the focus group consisted of two members from the RSRC having extensive expertise in the area of security and privacy for medical devices. The focus group members reviewed each proposition to reach a consensus to address the comments. In cases where focus group members were unable to reach a consensus for a proposition, revisit the development process of the respective code and key theme and update the proposition.

6.5 WBANSecRM framework – Expert Review Comments

The expert review of the WBANSecRM framework returned forty-nine comments. Table 6-3 presents the number of comments per category.

Table 6-3: No of comments per category

Category	No. of comments
Security and privacy risk analysis	10
Evaluate identified security and privacy risks	4
Security and privacy risk control	12
Overall evaluation of security and privacy risk controls	8
Usability and efficacy	8
General	7

6.5.1 Security and Privacy Risk Analysis

The security and privacy risk analysis category contains a total of 10 comments relating to the tools, techniques and methods presented in the WBANSecRM framework for identifying risks, threats and vulnerabilities. The expert review comments are presented in Table 6-4. These comments related to:

- List of threats and vulnerabilities
- New sources to identify threats and vulnerabilities
- Risk analysis approach
- Threat modelling tools and techniques
- Asset classification

Table 6-4: List of expert review comments for security and privacy risk analysis

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
List of threats and vulnerabilities	No Comment	I'm missing the following attack actions. Maybe they are covered, but I overlooked them. - Guessing passwords. (exploiting weak or default passwords) - Bypassing authentication, e.g. at the sensor device. (e.g. if authorization is done on a client)	No Comment	No Comment	Why are libraries not vulnerable to injection attacks? Side channels attack are missing
Threat and vulnerability sources	Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), U.S. National Vulnerability Database (NVD)	BSI Top 10 threats, OWASP Mobile Top 10 Other: Mitre ATT&CK for ICS.	No Comment	No Comment	No Comment
Risk analysis approach	Risk analysis should be applied as early as possible to avoid fundamental flaws in the security design whose removal in later lifecycle	No Comment	No Comment	No Comment	No Comment

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
	phases is very costly. As a consequence, risk analysis needs to be repeatedly applied in different phases, include risk aspects in the deployment and operation phases				
Threat modelling tools and techniques	No Comment	As said above, we derived our own method and tool, based on the requirements in ISO 27005, IEC 62443-4-1 and NIST 800-30.	The method and approach depend on the requirements of the domain, app, analysts, etc. There is no single one-size-fits-all approach. Probably STRIDE is the most known and applied though.	No Comment	1. STRIDE + LINDDUN are probably the most suitable methods as this provides methodological guidance and privacy knowledge support to systematically elicit and mitigate privacy threats in software architectures. 2. STPA-SafeSec might be an important additional method to mention
Asset classification	I noticed that the framework puts a strong focus on the security of data assets (and—to a lesser degree—of physical assets). What I missed was a mentioning of so-called processes assets, that is: functionality. Avoid to focus too narrowly on data assets. ISO/IEC TR 15446:2009 (a guideline closely related to the Common Criteria ISO/IEC 15408:2009) recommends to make an explicit distinction between information assets (data, code, config params), process assets (functionality), and physical assets (hardware)	No Comment	No Comment	No Comment	No Comment

List of threats and vulnerabilities: Expert 2 and expert 5 suggested adding four new threats which were not available in the Table Appendix E-1 list of threats and vulnerabilities for WBAN applications.

- Guessing passwords (exploit by using weak or default passwords)
- Bypassing authentication
- Injection attack
- Side-channel attack

Guessing passwords use in brute force attack to gain unauthorised access to a system. As brute force attack is already presented in the Table Appendix E-1, the focus group agreed not to add guessing passwords as an additional threat. **Bypassing authentication** use by an attacker to gain access to an authorised or privileged application, service, or device by evading or avoiding the authentication mechanism. Therefore, an attacker can access protected data without authentication. The focus group agreed to add the bypassing authentication threat for mobile and web applications in Table Appendix E-1. **Injection attack** allows an attacker to inject code into a program, query or inject malware on an application to run remote commands that can read or modify a database or modify data on a web application. Attackers use SQL Injection, Buffer Overflow, Cross-site scripting (XSS) and Code Injection to perform an injection attack. As SQL Injection, Buffer Overflow, Cross-site scripting (XSS), and Code Injection are already present in the WBANSecRM framework, the focus group agreed not to add injection attack as an additional threat. **Side-channel attack** (SCA) is a security exploit that attempts to extract information from a system. Side-channel attacks rely on measuring tendencies and frequencies of the hardware to establish patterns from which you can extract private information from the system. SCA can monitor the hardware's power use and electromagnetic emissions during cryptographic operations. The focus group agreed to add the side-channel attack for the sensor device in Table Appendix E-1.

Threat and vulnerability sources: Two experts' expert 1 and expert 2, recommended adding Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), U.S. National Vulnerability Database (NVD), BSI Top 10 threats, OWASP Mobile Top 10 and Mitre ATT&CK for ICS as additional sources to identify threats and vulnerabilities. The WBANSecRM framework already uses the 2021 CWE top 25, BSI Top 10 threats and OWASP Mobile Top 10 as sources to identify threats and vulnerabilities. The CAPEC is a collection of known cyber security attack patterns which cyber security professionals can use to understand how an attacker will exploit weaknesses in the applications.

The NVD is the largest and most comprehensive database of reported vulnerabilities of both commercial and open-source components. The NVD consists of a database of security checklists, software flaws, misconfigurations, and impact metrics which will help prevent security breaches. The focus group agreed with this comment to add NVD, CAPEC and Mitre ATT&CK for ICS sources in section 4.1.3.1 under Appendix B to identify the threats and vulnerabilities while performing risk analysis at the requirements analysis phase. The NVD database requires name, version and vendor of the software or product to search for the vulnerabilities, so an additional note was added in section 4.1.3.1 under Appendix B that organisations will require name, version and vendor of the software or product to search the NVD database.

Risk analysis approach: Expert 1 commented that risk analysis should be applied as early as possible to avoid fundamental flaws in the security design as removal of these flaws in later lifecycle phases is very costly. Consequently, risk analysis needs to be repeatedly applied in different phases, starting with the security/safety requirements, coarse-grained design and system architecture, the implementation, deployment, operation, and ultimately decommissioning the system under consideration. Currently, the WBANSecRM framework performs risk analysis in the requirements analysis and system architecture phases, so the focus group agreed to add a new step named *"Risks arising from risk control measures"* in section 4.2.2 under Appendix B. The purpose of this new step is to identify any new risk arising due to the selection and implementation of controls that mitigate risks. Post-production activities are out of the scope of the WBANSecRM framework, so the focus group agreed to consider risk analysis during the deployment and operation phase of the application as future work.

Threat modelling tools and techniques: Expert 2 commented that they derived their own method and tool based on the requirements in ISO 27005, IEC 62443-4-1 and NIST 800-30. The IEC 62443-4-1 standard provides the process requirements for the secure development of industrial automation and control systems products. The WBANSecRM framework also uses the requirements and guidelines provided by ISO 27005 and NIST 800-30. As the use cases of the industrial automation and control systems are not similar to WBAN based healthcare applications, the focus group agreed not to take any action to address this comment. Expert 3 commented that no single threat modelling tool and technique would fit all approaches. The method and approach needed depends on the requirements of the domain, app, and analysts. The expert also suggested that STRIDE is the best known threat modelling method. Expert 5 indicated that the combination of STRIDE and LINDDUN are probably the most suitable methods as this provides methodological guidance and privacy knowledge support to systematically elicit and mitigate privacy threats in software architectures. STRIDE is a developer-focused threat modelling method to identify the security threats in an application. STRIDE provides security threats in six categories: 1) Spoofing, 2) Tampering, 3) Repudiation, 4) Information disclosure (privacy breach or data leak), 5) Denial of service, and 6) Elevation of privilege. LINDDUN is a privacy threat modelling methodology that helps to identify and mitigate privacy risks in an application. Both STRIDE and LINDDUN use a data flow diagram (DFD) to identify security and privacy-related threats. The WBANSecRM framework aims to assure security and privacy, so the focus group agreed with the comment to consider STRIDE and LINDDUN as the most suitable threat modelling methods. A note is added in section 4.1.4.2 under Appendix B that STRIDE and LINDDUN are the most suitable threat modelling methods.

Expert 5 also suggested that STPA-SafeSec might be an essential additional threat modelling method. STPA-SafeSec examines the relationships between each system component, assuming that the system must be examined as a whole, considering all elements, from social to technical. The STPA-SafeSec methodology effectively overcomes problems that require both system safety and security. As modern applications are not static and evolve over time and are influenced by their socio and technical environment, STPA-SafeSec provides an iterative approach that can be reapplied throughout the system's lifetime. As the application's safety analysis is out of the scope of the WBANSecRM framework, the focus group agreed not to take any action for considering the STPA-SafeSec methodology to identify the safety and security hazards.

Asset classification: Expert 1 commented that the WBANSecRM framework puts a strong focus on the security of data assets and to a lesser degree on physical assets and process assets. A functionality view draws more attention to dynamic aspects; it may also reveal threats unrelated to data but related to behaviour. Assets associated with IT systems usually fall into three classes: a) information, b) processes, and c) physical (ISO 15446, 2017). Information assets represent data that is of value to an organisation. Process assets represent applications where data is transformed or analysed. The distinction between process assets and information assets is that the associated data is of little value without the processing capabilities of the related applications. Physical assets represent the information processing equipment used to support the information and process assets. The focus group agreed to classify the assets in three categories, information, process and physical, based on the guidelines provided by ISO 15446:2017. A note was added in section 4.1.3.1 under Appendix B detailing each asset classification, which will guide the organisation during the asset identification process.

List of changes made after reviewing the expert review comments for the security and privacy risk analysis category :

- Added a note that STRIDE and LINDDUN are the most suitable threat modelling methods.
- Added bypassing authentication and side-channel attack in the list of threats and vulnerabilities.
- Added the types of asset categories that need to be considered while identifying the assets.

- Added a note that organisations can use a binary approach as an alternative approach instead of impact or likelihood for evaluating the risk.
- Added Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), U.S. National Vulnerability Database (NVD), BSI Top 10 threats, and Mitre ATT&CK for ICS as additional sources to identify the threats and vulnerabilities.
- Added an explanatory sentence for conducting risk analysis in every phase of the development lifecycle as an iterative process.

6.5.2 Evaluate Security and Privacy Risks

The evaluate security and privacy risks category contains 4 comments relating to the process to determine whether the risks identified in the security and privacy risk analysis step are acceptable or not. The expert review comments are presented in Table 6-5. These comments related to:

- Risk evaluation process
- Risk priority approach

Table 6-5: List of expert review comments for evaluate security and privacy risk

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Risk evaluation process	Neither impact nor likelihood can be precisely quantified for potential security incidents. Therefore, I rather tend to treat security risks as binary events; they are either possible or impossible.	Likelihood is my view best structured into several factors, like exposure and exploitability.	Impact and likelihood are general concepts that are used for risk assessment.	No Comment	No Comment
Risk Priority approach	Once the list of potentially possible risks has been determined, the risks can be simply ordered relative to each other by expert consensus, rather than assigning absolute priorities to each individual risk. Risks are not eliminated in the order of their priority, anyway. Often, different risks have a common root cause, and by eliminating this root cause, several risks with completely different priorities can be removed in one step. Therefore, I would not put too much emphasis on risk ranking—a very coarse-grained approach is probably "good enough" in practise.	No Comment	No Comment	No Comment	No Comment

Risk evaluation process: Expert 2 commented that likelihood is best structured as likelihood can be further broken down into exposure and exploitability of the risk. Expert 3 commented that impact and likelihood are general concepts used for risk assessment. Expert 1 commented that neither impact nor likelihood could be precisely quantified for a potential security incident. Expert 1 proposed using a binary approach *"possible"* or *"impossible"* instead of impact or likelihood. The focus group agreed with expert 1's comment to consider the binary approach as an alternative way to evaluate the risk instead of calculating impact and likelihood. To address expert 1's comment, section 4.1.3.2 under Appendix B was amended to include that organisations can use a binary approach as an alternative to evaluating the risk.

Risk Priority approach: Expert 1 commented that once the list of potential risks has been determined, the risks can be prioritized by taking expert consensus, rather than assigning absolute priorities to each risk. Although the WBANSecRM framework recommends prioritising risk controls based on the risk score value, the focus group agreed with the comment that organisations could alternatively prioritise the risk control based on expert consensus or product delivery plans. To address the comment, a note was added in section 4.2.3 under Appendix B that organisations can use expert consensus to prioritise the risk controls based on the relationship between multiple risks mitigated by one or more control.

List of changes made after reviewing the expert review comments from the evaluate security and privacy risks category:

- Added an explanatory sentence in the risk evaluation section that results from likelihood and impact analysis will be subjective.
- Added an explanatory sentence in the risk evaluation section to use expert consensus as an alternative approach for the risk priority, if the organisation has an expert resource

6.5.3 Security and Privacy Risk Controls

The security and privacy risk controls category contains 12 comments relating to selecting security and privacy controls, along with each control's implementation detail. The expert review comments are presented in Table 6-6. These comments related to:

- The WBANSecRM framework consists of the appropriate risk controls
- Whether the risk controls have adequate implementation details
- Sources used to develop the risk control implementation details
- Testing methods used during implementation of the risk control

Table 6-6: List of expert review comments for security and privacy risk control

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Risk control	They definitely contribute to the goal of achieving security and privacy assurance.	1. The list of threats is pretty comprehensive. 2. The security control could be more targeted. If the threat is not described more specifically, then the table could be arranged in a more concise way. But I think it would be very useful to adapt the threat description for the asset and sub-asset	No Comment	No Comment	1. It's a great start but such a list can never be complete – neither in terms of attack vectors nor in terms of mitigation. 2. Add Hardware Security Modules, Confidential Computing as control
Risk control source	FDA regulation for the US market; EU regulations about healthcare products or medical devices within Europe (e.g., EU Regulation 217/745), Common Criteria Part 2, 21 CFR Part 11	IEC 62443 4-2	Autodesk continuous threat modelling – developer checklist	No Comment	No Comment
Lack of implementation details	No Comment	No Comment	Some are not really targeted at developers. For instance, the first bullets for access control seem more like organizational guidelines (define an access control policy…)	No Comment	Add pointers to reference implementations and technologies that help with implementing the control.
Testing and review methods	In safety- engineering, usability testing is an important element to see whether the users tend to misuse the system or do not understand the intention behind certain safeguards. Depending on the complexity and criticality of an application	No Comment	No Comment	No Comment	No. You mention integration testing, vulnerability scanning and pen testing earlier in the document – why are these dropped later?

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
	and its security controls, security usability may also become a relevant factor to exclude “human factors” as sources of risk.				

Risk control: Expert 1 commented that the controls presented in Table Appendix E-1 definitely contribute to the goal of achieving security and privacy assurance. Expert 2 commented that the list of threats and vulnerabilities with respective controls presented in Table Appendix E-1 is pretty comprehensive. Expert 2 also recommended providing the threat description for each asset and sub-asset to make the control more targeted. The threat description will explain how the asset and sub-asset will be affected if the attacker launches an attack. However, developing the threat description for each asset and sub-asset is a time-intensive task. Due to time limitations, the focus group agreed to consider providing the threat description for each threat asset and sub-asset as future work of this study.

Expert 5 commented that such a list could never be complete neither in terms of attack vectors nor in terms of mitigation. The WBANSecRM framework suggests that developer can use the list as a starting point. Additionally, the WBANSecRM framework also provide the steps to find a control to mitigate the new threats and vulnerabilities. Expert 5 also commented on considering Hardware Security Modules and Confidential Computing as an additional control. A hardware security module (HSM) is a physical computing device that protects and manages digital keys, conducts encryption and decryption for digital signatures, and performs other cryptographic functions. The Confidential Computing control will help to isolate sensitive data in a protected CPU enclave during processing. In a cloud environment, the processed data from the confidential computing will only be accessible from authorised program code. The focus group agreed with the comment to add Confidential Computing as an additional control as the WBANSecRM framework already recommends the use of Hardware Security Modules as part of key management control.

Risk control sources: Expert 1 suggested using the following sources for identifying the risk controls and respective implementation details which are recommend by the FDA, EU regulations about healthcare products or medical devices (e.g., EU Regulation 217/745), Common Criteria Part 2 and 21 CFR Part 11. The WBANSecRM framework used ISO/IEC 80001-2-2, NIST 800-53, ISO 27002, ISO 27799, ISO/IEC 11770, NIST 800-175B, NIST 800-56A, RFC 6749, and OWASP. These standards are recommended by the FDA, HIPAA and EU MDR to identify the security and privacy controls and respective implementation details. Expert 2 suggested the use of IEC 62443-4-2 as an additional source for identifying controls. The IEC 62443-4-2 standard provides security requirements for industrial automation and control systems, whereas the goal of the WBANSecRM framework is to provide risk controls for WBAN based healthcare application. For this reason, the focus group did not agree with expert 2’s recommendation to use IEC 62443-4-2 as a source to identify risk controls.

Expert 3 recommended using *Autodesk continuous threat modelling – secure developer checklist* as an additional source. The recommended source outlines authentication, authorisation, input validation, key management, system hardening and audit log as risk controls for embedded systems. Furthermore, the recommended source also presents the implementation details for the above risk controls which will assist the developer to implement the risk control. For this reason, the focus group agreed with this comment and agreed to amend the list of additional sources in section 4.2.5 under Appendix B.

Lack of implementation details: Expert 3 and expert 5 commented that the WBANSecRM framework does not contain adequate details for implementing risk controls. The other three experts think the WBANSecRM framework consists of appropriate implementation details for security and privacy risk controls. Expert 3 commented that some control implementation details are not targeted for developers and recommended grouping them together with related organisational policies. For instance, the first bullet of the access control seems more like organisational guidelines. The focus group agreed with the comment to update the control's implementation details, which contain both policy and development guidelines. The implementation details for access control and key management were amended by grouping policy-related guidelines. Expert 5 recommended adding pointers to reference implementations and technologies that could help with implementing the control. To address this comment, a working example or code snippet needs to be provided for each of the risk controls in the context of popular programming languages. The working example or code snippet will assist the developer during implementation of the risk control. To develop these working examples or code snippets for each risk control would require considerable time. Due to time constraints the focus group agreed to consider this as future work of this study.

Testing and review methods: The WBANSecRM framework recommended using code review and unit-testing as testing and review approaches during the control implementation phase. Expert 1 commented that in safety- engineering, usability testing is an important element to see whether the users tend to misuse the system or do not understand the intention behind certain safeguards. Depending on the complexity and criticality of an application and its security controls, security usability may also become a relevant factor to exclude “human factors” as sources of risk. The focus group agreed with the comment as usability testing is a method of determining whether a particular medical device meets the needs and preferences of its intended users. Usability testing helps uncover opportunities to make medical devices easier, safer, more effective, and more enjoyable to use. IEC 62366-1 is an international standard that helps medical device manufacturers to consider human factors by providing a standardised procedure for the analysis, specification, development and evaluation of the usability of their medical devices. So, the focus group agreed to amend section 4.2.4 under Appendix B to state that organisations also need to perform usability testing during the verification of the security and privacy controls in the implementation phase. To conduct the usability testing organisations can follow the guidelines provided by IEC 62366-1.

Expert 5 commented that "*No. You mention integration testing, vulnerability scanning and pen testing earlier in the document – why are these dropped later?*". The WBANSecRM framework proposed conducting software integration testing after implementing the security and privacy controls. Software integration testing is a level of software testing where individual units are combined and tested as a group. Integration tests help to identify whether independently developed units of software work correctly when they are connected to each other. The WBANSecRM framework recommends using Black Box Testing, White Box Testing, and Gray Box Testing methods to conduct integration testing. The WBANSecRM framework also recommends that during software integration testing, the developer needs to conduct two key tests:

- Security and privacy requirements testing - to validate the security and privacy requirements identified during the security risk assessment steps are implemented properly. This can be achieved by conducting functional, performance and scalability testing
- Threat and vulnerabilities mitigation testing - to validate the effectiveness of the implemented security controls against the identified threats and vulnerabilities

Furthermore, the WBANSecRM framework also recommends using vulnerability scanning and/or penetration testing to assess the overall residual security and privacy risk of an application upon completion of the security and privacy risk control implementation and verification stage. The comment was not clear to the focus group, and a follow-up email was sent to the respective reviewer for more context. The reviewer did not reply with more details, so the focus group agreed not to take any further action to address this comment.

List of changes made after reviewing the expert review comments from the security and privacy risk controls category:

- Added an explanatory sentence that the effectiveness of the control will depend on the circumstances, the business goals, the types of hardware and software components and their failure modes, and on the criticality of the specific requirements for the application.
- Added Autodesk continuous threat modelling – developer checklist as an additional source to identify risk control implementation details.
- Added a new sub-section as a step to evaluate risks arising from the selected risk control measures.
- Added a note that organisations also need to perform usability testing during the verification of the security and privacy control in the implementation phase. To conduct the usability testing organisations can follow the guidelines provided by IEC 62366.

6.5.4 Evaluation of Security and Privacy Risk Controls

The evaluation of security and privacy risk controls category contains 8 comments related to:

- Whether the approach is adequate to evaluate the security and privacy risk level of the application.
- Identify alternative approaches which could be used instead of penetration testing and/or vulnerability scanning as recommended in the WBANSecRM framework.

Table 6-7 illustrates the list of expert reviewer comments for evaluation of security and privacy risk controls.

Table 6-7: List of expert review comments for evaluation of security and privacy risk controls

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Techniques for evaluation of security and privacy risk controls	1. The required scrutiny is dictated by the safety-, security- and privacy-criticality of the application. For a simple fitness tracker that does only record few parameters and little to no person-identifiable information,	1. Penetration testing is useful if a very high level of assurance is required. It contains more advanced security testing than vulnerability scanning. 2. Checks for secure configuration and hardening	Both will be required to check the implemented security measures	Their combination is effective in offering a cost-scaled solution towards addressing both common weaknesses, as well as application-specific ones for	1. Pen testing is much more in depth and will usually include vulnerability scans. Whether both are necessary depends a lot on the use case and the identified risks and their classification.

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
	reduced effort seems feasible. If I had to choose in such cases, I would opt for vulnerability scanning rather than penetration testing, because the latter is closer to "testing security into the system" instead of "security by design". Of course, if time and budget allow for it: More is always better. 2. An assessment of user-friendliness of security and privacy controls to avoid threats caused by human factors			a given application.	2. Depending a lot on the use case and the risks classification: Formal verification techniques, independent security assessment.

Techniques for evaluation of security and privacy risk controls:

Expert 1 commented that he would choose vulnerability scanning instead of penetration testing for a simple fitness tracker that only records a few parameters and little to no personally identifiable information. Expert 1 also commented that vulnerability scanning and penetration testing would be better if the time and budget allowed. Expert 2 commented on using penetration testing over vulnerability scanning as penetration testing provides a very high level of assurance. Expert 2 also commented that penetration testing contains more advanced security testing than vulnerability scanning. Experts 3 and 4 commented that vulnerability scanning and penetration testing would be required to check the implemented controls. Expert 5 commented on using penetration testing as penetration testing provides much more in-depth testing and usually includes vulnerability scanning. In summary, the options recommended by the reviewers are:

- Choose penetration testing as it will provide a very high level of assurance and in-depth testing of the implemented controls;
- Choose only vulnerability scanning if the application only records a limited number of parameters without personally identifiable information;

- Choose both penetration testing and vulnerability scanning if time and budget allow.

According to the AAMI TIR 57 standard, an organisation can employ testing techniques such as vulnerability scans and/or penetration testing to evaluate an application's overall residual security and privacy risk. However, selecting suitable testing techniques for evaluation of security and privacy risk controls is challenging task for the organisations. So, the focus group agreed to amend the section 4.3 under Appendix B with the above possible options. This will assist the organisation in selecting the appropriate testing method.

Expert 1 suggested conducting an assessment of the user-friendliness of security and privacy controls to avoid threats caused by human factors. Security and privacy need to work alongside the usability of the application. Assuring security and privacy of applications cannot dictate the usability of the application. For example, forcing users to use very long and complex passwords as part of the authentication process might downgrade the usability of the application. Usability tests involve recruiting users of a specific user group and observing them while performing tasks with the medical device. Usability tests are typically conducted in simulated-use conditions that could affect how the users interact with the medical device. Usability tests can be conducted on one or more prototypes with varying degrees of options, such as paper sketches, wireframes, hardware or software mock-ups, a functional prototype, or a completed medical device. The focus group agreed to amend section 4.2.4 under Appendix B so that the organisation can perform usability testing during the security and privacy control implementation phase or once the application is ready. To conduct the usability testing, organisations can follow the guidelines provided by IEC 62366-1.

Expert 2 recommended conducting an assessment of the secure configuration and hardening of the application. Improper configuration of the assets used to develop the application will increase the risk of security and privacy breaches of the application. Additionally, it is often seen that organisations rush to deploy the application in production with default settings without implementing basic hardening. So, the focus group agreed with the comments to add a note in section 4.3 under Appendix B that organisations need to conduct a secure configuration and hardening assessment in addition to penetration testing and/or vulnerability scanning.

Expert 5 recommended the use of formal verification techniques and independent security assessments as additional approaches to evaluate the security and privacy controls. Formal verification is a security audit method for proving the correctness of underlying algorithms in terms of a formal specification. Formal verification provides a systematic approach to identifying the flaws of a protocol. To perform formal verification within the WBANSecRM framework, it is required to design the formal specification for each control presented in the WBANSecRM framework. Developing formal specifications for each control is time-intensive work. Due to time constraints, the focus group agreed to consider this as future work of this study. Expert 5 also suggested using independent security assessment during the evaluation of security and privacy risk controls. As the WBANSecRM framework already recommends that organisations can use independent security assessment by onboarding a third-party service provider, so the focus agreed that no action is required for this comment.

List of changes made after reviewing the expert review comments from evaluation of security and privacy risk controls category:

- Added possible criteria which will assist the organisation in selecting the appropriate method for evaluating the overall residual security and privacy risk.
- Added a note for checking secure configuration and hardening in addition to penetration testing and/or vulnerability scanning.

6.5.5 Usability and Efficacy

To determine the WBANSecRM framework’s usability and efficacy the experts were asked four separate questions. Questions 1 and 2 were asked to determine the usability of the

WBANSecRM framework, followed by question 3 to determine its efficacy. Additionally, question 4 was asked to check whether the reviewer would consider the WBANSecRM framework while developing WBAN based healthcare applications. The questions and responses are shown in Table 6-8.

Table 6-8: Responses to the WBANSecRM framework Usability and Efficacy

No	Questions	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
1	Is it easy to understand and follow the proposed framework?	Very Easy	Neither	Difficult	Easy	Neither
2	Do you think this framework has sufficient detail for a developer to use?	Yes	Yes	Yes/No	Yes	No
3	In your opinion how effective is the framework in assuring security and privacy of WBAN applications?	Effective	Neither effective or ineffective	Effective	Very Effective	Neither effective or ineffective
4	Would you consider the proposed framework if you are planning to develop a WBAN based healthcare application?	Yes	Yes/No	Yes	Yes	Yes

The table indicates the response to question 1, *"Is it easy to understand and follow the proposed framework?"*. Two experts (1 and 4) think the WBANSecRM framework is easy to understand, two experts (2 and 5) think it is neither easy nor difficult to follow the WBANSecRM framework. Expert 2 commented that the document contains inconsistent terminology while presenting the figures and describing the steps. Expert 3 commented that *"it feels too academic for a user-friendly tutorial document"*. In response to question 2, three experts (1, 2 and 4) think the WBANSecRM framework has sufficient detail for the developer. Expert 3 replied with an inconclusive response by selecting both yes and no options. Expert 3 also commented that *"The level of detail might be ok, but the list can be overwhelming"*. Additionally, expert 5 thinks the WBANSecRM framework is not targeted for the developer with the comment: *"The document appears to be targeting analysts and consultants rather than developers and testers. A fully worked-out example application would be a nice addition as an appendix"*. In total, eight comments from experts are categorised and presented in Table 6-9.

Table 6-9: List of expert review comments for usability and efficacy of WBANSecRM framework

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Structure of the document	No Comment	No Comment	1.It feels too academic for a user-friendly tutorial document 2. I would suggest to extend this text with your rationale and references, and then distill a separate guide/tutorial document from this document for people to actually use in practice. (this document can be overwhelming)	No Comment	1. Document structure could be improved. Frequent jumps to the appendices and back do not improve comprehension. 2. The document appears to be targeting analysts and consultants rather than developers and testers. A fully worked-out example application would be a nice addition as an appendix
Security and Safety relationship	In the healthcare domain, in particular, security is often just a secondary issue, but the main concern is safety. Thus, the emphasis of a security evaluation is often on »security for safety«, because security incidents may jeopardise the safety of the system, sometimes with severe medical implications. Therefore, it would be nice to have an integrated risk management framework that is able to handle both safety and security risks.	No Comment	No Comment	Lack of detail in the discussion between the security and safety lifecycle; it would seem prudent to more carefully consider the interaction between the lifecycles and aim to discover safety-critical issues earlier rather than later, as the latter are typically more important to address, both from a regulatory, as well as development-cost perspective	The framework completely ignores safety and interactions between safety engineering and security/privacy engineering.
Efficacy to cover privacy	No Comment	I do not quite see how the framework covers privacy.	No Comment	No Comment	No Comment

Structure of the document: Expert 3 commented that it feels too academic for a user-friendly tutorial document. Additionally, expert 5 commented that frequent jumps to the appendices and back make it hard to follow. As the WBANSecRM framework document was written as part of a research study, the focus group agreed to create a web version of the WBANSecRM framework as future work. The web version of the WBANSecRM framework will provide easy navigation to the different chapters and appendices of the WBANSecRM framework. Expert 3 also commented on adding a note for the user on how to use the WBANSecRM framework.

Additionally, expert 5 commented that a fully worked-out example would be a nice addition as an appendix. Although the WBANSecRM framework contains a worked example for developing WBAN based healthcare applications which is presented in Appendix D, it was not outlined in the *Executive Summary* or *Scope* section. A new section named *"How to use the framework"* was added at the beginning of WBANSecRM framework, to make the worked-out example more visible to the user.

Security and Safety relationship: Expert 1, expert 4 and expert 5 commented that the WBANSecRM framework completely ignores the interactions between safety engineering and security and privacy engineering. Expert 1 also commented that it would be nice to have an integrated risk management framework to handle safety and security risks. In Clause 4.2 of ISO 62304 it is recommended that healthcare software manufacturers should establish the following two processes as part of risk management (IEC 62304, 2019):

- A safety process for identifying hazards, managing risks, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the risk controls in compliance with ISO 14971
- A security process for managing risks associated with security which include identifying vulnerabilities, estimating and evaluating the associated threats, controlling these threats, and monitoring the effectiveness of the risk controls

ISO 62304 also recommends that organisations can use the above approaches as two separate processes or combine them as a single process. Additionally, AAMI TIR 57 suggests using two separate processes to manage safety risks, and security and privacy risks due to the following reasons:

- The risk associated with system and data security might not lead to harm as narrowly defined in ISO 14971;

- The risk of compromising the confidentiality, integrity and availability of protected health information that is not considered harmful in the context of ISO 14971;
- Business and reputation risks due to a security and privacy breach are not deemed harmful to the safety sense;
- When security risks lead to safety risks, security and safety personnel must work jointly to contribute to the analysis of security risks and to transfer any safety-related risks identified during security analysis to safety analysis;
- A separate risk analysis process will only focus on impacts identified by a security and privacy analysis.

As the WBANSecRM framework was developed to assure security and privacy of a WBAN based healthcare application, mitigating safety-related risks is out of the scope of this study. Based on the above recommendations and considering the scope of this research study, the focus group agreed not to take any further action to address the comment. Furthermore, a note was added in section 4.2 under Appendix B that organisations need to conduct safety risk analysis in parallel based on the guidelines provided by ISO 14971.

Efficacy to cover privacy: Expert 2 commented that he does not see how the WBANSecRM framework covers privacy. The current version of WBANSecRM framework addresses privacy in the following ways:

1) Provides a list of security and privacy requirements which organisations can use as a starting point;
2) Provides strong emphasis on using access control, authentication, anonymisation, non-repudiation and authorisation to restrict unauthorised access to data;
3) Provides cryptographic control to encrypt the data at rest and while in transit;
4) Recommends using an audit log and accountability control to perform auditing and make users accountable for their unauthorised action.

A follow-up email was sent to Expert 2 to get more context about the comment. However, the reviewer did not reply with any more details. In addition to the above measures, the focus group agreed to consider a threat modelling framework which will help to identify the privacy-related risk. LINDDUN is a threat modelling framework which provides a systematic approach to eliciting and mitigating privacy-related threats in a software system. LINDDUN helps developers with limited privacy expertise to assure privacy early in the software development life cycle. LINDDUN provides both model-based and knowledge-based approaches to identify and mitigate threats. The model-based approach systematically uses a data flow diagram (DFD) to examine each DFD component for privacy threats. The knowledge-based approach provides an overview of the most common attack paths related to Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance. So, LINDDUN as a threat modelling method was added along with STRIDE to identify the privacy-related risk, while conducting risk analysis in the system architecture phase.

List of changes made after reviewing the expert review comments from the usability and efficacy category:

- Added a new section named "How to use the framework" was added at the beginning of WBANSecRM framework, to make the worked-out example more visible to the user.
- Scope section was amamended and added a note that safety risk management and post-production activities are set out of the scope while developing the WBANSecRM framework.
- Added an explanatory sentence that organisations need to conduct safety risk analysis in parallel based on the guidelines provided by ISO 14971.

6.5.6 General

The general category contains 7 comments related to:

- Whether there are any typographical errors in the WBANSecRM framework;

- Whether any references need to be included in the WBANSecRM framework;
- Whether terminology is inconsistent in the WBANSecRM framework;
- Whether any explanatory sentences are required explaining the rationale.

Table 6-10 illustrates the list of expert reviewer comments for the General category.

Table 6-10: List of expert review comments for general category

Sub-category	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
Typographical error	No Comment	No Comment	There are typos in almost every picture	No Comment	No Comment
Lack of academic references	No Comment	Is there a reference for the description of the security risk assessment approach?	It lacks academic references	No Comment	No Comment
Inconsistent terminology	No Comment	1. Is Fig 1 following a specific methodology, i.e. what is the meaning of the (rounded) rectangles? I could not detect a separation of actions and outputs. 2. 'Security risk evaluation and treatment' is now one box, while there were different boxes in Fig 2. This is confusing for the reader.	No Comment	No Comment	No Comment
Explanatory sentence with rationale	No Comment	No Comment	1. Explanation of how you created it (why did you choose certain things, what framework(s) do these come from, etc.) 2. Some parts of this assessment feel a bit ad-hoc/ subjective. (This interpretation might be wrong. In that case, adding some rationale why it is done in this way could help)	No Comment	No Comment

Typographical error: Expert 3 commented that there are typos in almost every picture. The focus group agreed with the comment and all the figures have been revisited to fix the typographical errors.

Lack of academic references: Expert 3 commented that the document lacks academic references. The focus group agreed with the comment and added references for the ISO/IEC 80001-2-2, ISO/IEC 80001-2-8, NIST 800-53 and ISO/IEC 27002, ISO 27799 standards. Expert 2 commented to add a reference for the description of the security risk assessment approach. The focus group agreed with the comment and added reference in section 4.1.2 under Appendix B.

Inconsistent terminology: Expert 2 commented that the document contains inconsistent terminology while presenting the figures and describing the steps. Expert 2 also commented that figures consist of normal rectangles and rounded rectangles, making it hard to separate the action and output. The focus group agreed with these comments and agreed to use normal rectangles for actions and rounded rectangles for outputs. All figures were redrawn to address these comments. Additionally, inconsistent terminology such as *"risk control"* and *"security risk control"* was changed to *"security and privacy risk control"*.

Explanatory sentence with rationale: Expert 3 suggested "*adding an explanatory note with rationale for why certain things were chosen*". The focus group agreed with the comment, and an explanatory note with rationale was added in section 3 of Appendix B for selecting standards, the risk assessment approach and calculating the risk score using impact and likelihood.

List of changes made after reviewing the expert review comments from the usability and efficacy category:

- Figure Appendix B- 1 was redrawn and typos fixed.
- Added rationale for selecting the ISO/IEC 80001-2-2, ISO/IEC 80001-2-8, NIST 800-53 and ISO/IEC 27002 standards.
- Added references for the ISO/IEC 80001-2-2, ISO/IEC 80001-2-8, NIST 800-53, ISO/IEC 27002, and ISO 27799 standards.

6.6 Changes to the WBANSecRM Framework As a Result of Expert Review

The security and privacy risk analysis section was amended to include the following:

- Added a note that STRIDE and LINDDUN are the most suitable threat modelling methods;
- Added bypassing authentication and side-channel attack in the list of threats and vulnerabilities;
- Added the types of asset categories that need to be considered while identifying the assets;
- Added a note that organisations can use a binary approach as an alternative approach instead of impact or likelihood for evaluating the risk;
- Added Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), U.S. National Vulnerability Database (NVD), BSI Top 10 threats, and Mitre ATT&CK for ICS as additional sources to identify the threats and vulnerabilities;
- Added an explanatory sentence for conducting risk analysis in every phase of the development lifecycle as an iterative process;
- Added an explanatory sentence in the risk evaluation section that results from likelihood and impact analysis will be subjective;

The security and privacy risk controls section were amended to include the following:

- Added an explanatory sentence that the effectiveness of the control will depend on the circumstances, the business goals, the types of hardware and software components and their failure modes, and on the criticality of the specific requirements for the application;
- Added *Autodesk continuous threat modelling – developer checklist* as an additional source to identify risk control implementation details;

- Added a new sub-section as a step to evaluate risks arising from the selected risk control measures;
- Added an explanatory sentence in the risk evaluation section to use expert consensus as an alternative approach for the risk priority, if the organisation has an expert resource;
- Added a note that organisations also need to perform usability testing during the verification of the security and privacy control in the implementation phase. To conduct the usability testing organisations can follow the guidelines provided by IEC 62366;

The evaluation of the overall residual security and privacy risk acceptability section was amended to include the following:

- Added possible criteria which will assist the organisation in selecting the appropriate method for evaluating the overall residual security and privacy risk;
- Added a note for checking secure configuration and hardening in addition to penetration testing and/or vulnerability scanning;

The scope was amended to include the following:

- Safety risk management and post-production activities are set out of the scope while developing the WBANSecRM framework;
- Added an explanatory sentence explaining the rationale for selecting the ISO 62304 standard;

The overview section was amended to include the following:

- Figure Appendix B- 1 was redrawn and typos fixed;
- Added rationale for selecting the ISO/IEC 80001-2-2, ISO/IEC 80001-2-8, NIST 800-53 and ISO/IEC 27002 standards;

- Added references for the ISO/IEC 80001-2-2, ISO/IEC 80001-2-8, NIST 800-53, ISO/IEC 27002, and ISO 27799 standards.

6.7 List of Future Work for WBANSecRM Framework As a Result of Expert Review

The list of future work identified for the WBANSecRM framework as a result of expert review are presented below:

- In order to improve the usability of the WBANSecRM framework, creating a web version of the WBANSecRM framework would provide easy navigation to the different chapters and appendices of the WBANSecRM framework.
- Formal verification provides a systematic approach to identifying the flaws of a protocol. To perform formal verification within the WBANSecRM framework, it is required to design the formal specification for each control presented in the WBANSecRM framework. Developing formal specifications for each risk control is considered future work of this study.
- A threat description explains how the asset and sub-asset will be affected if the attacker launches an attack. But, developing the threat description for each asset and sub-asset is a time-intensive task. Due to time limitations, providing the threat description for each threat asset and sub-asset is left for future work.
- A worked example or code snippet will assist the developer during the implementation of the risk control. Developing these worked examples or code snippets for each risk control would require considerable time. Due to time constraints in developing a worked example or code snippet for each risk control, this is considered as future work of this study.

6.8 Summary

This chapter describes the approach taken to validate the WBANSecRM framework using expert review. The expert review was completed in five stages. The first stage was to develop the questionnaire, which resulted in twenty questions, followed by recruiting appropriate experts. The questionnaire and beta version of the WBANSecRM framework were then presented to five experts for review. After receiving the completed questionnaires, the 49 comments received from the experts were analysed to ascertain the usability and efficacy of the WBANSecRM framework. Once the analysis was complete, the comments and propositions to address the respective comments were reviewed by a focus group. Finally, the focus group reviewed the experts' comments and the suggested changes, and through discussion, a consensus was reached on which changes should be adopted.

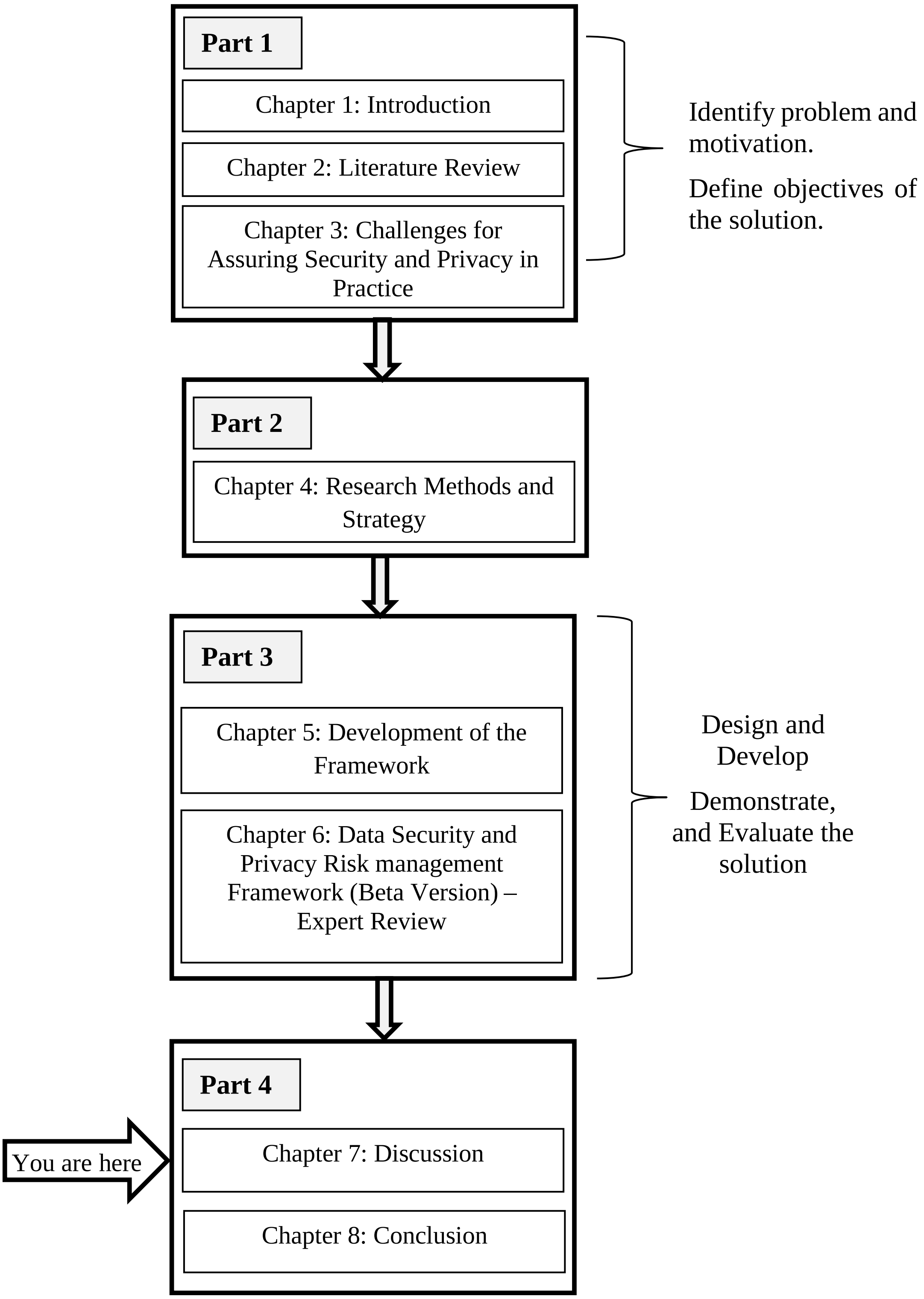
The focus group analysis of the 49 reviewer comments resulted in 19 changes, as detailed in section 6.6. The major changes include types of asset categorisations that need to be considered while identifying the assets. Additionally, STRIDE and LINDDUN are recommended as the most suitable threat modelling methods, followed by CWE, CAPEC and NVD database, which is added as an additional source to identify the threats and vulnerabilities. Furthermore, a new sub-section was added to evaluate risks arising from the selected risk control measures. An explanatory note was added that organisations could use a binary approach as an alternative approach instead of impact or likelihood for evaluating the risk. Finally, possible criteria were presented to assist the organisation in selecting the appropriate method for evaluating the overall residual security and privacy risk.

Five comments were accepted by the focus group but were not implemented due to time constraints and were considered future work. To address these five comments, four changes were identified, as detailed in section 6.7. Among them was creating a web version of the WBANSecRM framework to improve its usability. Additionally, to make the WBANSecRM framework more developer-friendly, formal specifications for each risk control should be developed. Furthermore, developing the threat description for each asset and sub-asset which will explain how the asset and sub-asset will be affected if the attacker launches an attack.

The purpose of the expert review was to evaluate the usability and efficacy of the WBANSecRM framework. Four experts think the WBANSecRM framework has sufficient detail for the developer. One of the above four experts also think the level details might be ok, but this list can be overwhelming. Expert 1 and 3 think the WBANSecRM framework will be effective, followed by expert 4 who thinks the WBANSecRM framework will be very effective in assuring the security and privacy of WBAN applications. Four experts (experts 1, 3, 4, 5) think they would consider using the WBANSecRM framework if they were planning to develop a WBAN based healthcare application. Expert 2 commented that the document needs to be improved by adding more rationale, adding explanatory sentences and improving the document structure. To address the comment, more rationale and explanatory sentence was added in different sections of the document.

The next chapter reviews the overall study, revisiting the research questions and objectives, and examines the research threat to validity.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
You are here
Chapter 7: Discussion
Chapter 8: Conclusion

7 Discussion

7.1 Introduction

Developing WBAN healthcare applications is a complex process that requires careful attention to security and privacy concerns. The protection of PHR data is of the utmost importance. This research aims to provide developers with a framework to help them create applications that comply with regulations and prioritise data security and privacy. This chapter discusses how the framework can help to assure security and privacy in WBAN-based healthcare applications. It also highlights the implications of these findings, which can be valuable for both theoretical and practical purposes.

7.2 Research Objectives and Question Revisited

As outlined in the introduction chapter of this thesis, this study aims to investigate *"How can the development of a wireless body area network (WBAN) data security and privacy risk management framework for healthcare applications assist developers and organisations in improving the security and privacy of data, and put them on the road to regulatory compliance?"*

In order to meet this aim, the following two research objectives were developed:

> *RO 1: To design and develop a Data Security and Privacy Risk Management Framework which will assist developers in assuring security and privacy of WBAN based healthcare applications.*
>
> *RO 2: To validate the Data Security and Privacy Risk Management Framework.*

Sections 7.2.1 and 7.2.2 present how each of these two objectives was fulfilled.

7.2.1 Objective 1

A literature review was conducted to investigate the challenges faced by developers while developing a WBAN based application. The literature review revealed various challenges for

WBAN applications including energy efficiency, antenna design, quality of service and, security and privacy. To corroborate these challenges, an interview was conducted with a WBAN development organisation. The organisation indicated that while each of the above challenges existed for them, concerns around implementing security and privacy were at the forefront. They stated that they have a high demand for data security and privacy because their product collects and analyses PHR data. The list of challenges faced by developers for assuring security and privacy identified from both the literature review and interview are presented below:

- Lack of trained staff, budget, and management support
- Limited knowledge about market-specific regulatory requirements and security standards, policies and goals
- The existing standards outline what to do but do not provide adequate details for how to implement
- Lack of comprehensive understanding of the architecture for WBAN security and privacy
- Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage
- Lack of information about the threats related to permission, privileges and access control during system operation
- Standards outline each control at a very high-level with a limited amount of implementation detail
- Identifying and implementing appropriate security and privacy controls to assure data confidentiality, integrity and availability
- Due to the vast number of controls, the challenge is prioritizing these controls in addition to planning releases without compromising security and privacy

Discussion

The literature review indicates that a WBAN application can be affected by a total of eleven types of attack. Denial-of-service, eavesdropping, replay attacks, and data modification attacks are the most common attacks for WBAN applications. The literature review also indicates that there are twenty-two types of requirements to assure the security and privacy of WBAN applications. The most referenced security and privacy requirements are data confidentially, data integrity, data availability, authentication, encryption, data privacy, key management and access control. The least addressed security and privacy requirements are a firewall, physical protection, auditing, client platform security, and anonymity.

The literature review also indicates that none of the existing solution approaches addresses all the security and privacy requirements. Various standards and guidelines propose lists of security and privacy controls for implementing proper safeguards of PHR data. Due to the vast lists of security and privacy controls with lack of implementation details, implementation of these controls is complex and challenging. The literature review also indicates that existing risk management frameworks for healthcare applications were primarily developed for applications which operate within a healthcare delivery organisation's IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media. When a WBAN application operates in an environment where many people have open internet access, this leaves them vulnerable and open to many types of attacks and threats. Additionally, open connectivity creates a large attack surface. WBAN applications consist of resource constrained sensor devices which have limited memory and computational power and the literature review indicates that none of the frameworks provide guidance for managing security and privacy risks for resource-constrained sensor devices.

The FDA recognises that the security and privacy of medical devices is a shared responsibility among stakeholders, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices (FDA, 2020). Medical devices should be designed to protect assets and functionality and reduce the risk of loss of authentication, availability, integrity, and confidentiality. Title 21 CFR part 820 - Quality System Regulation states that the medical device manufacturer must employ a cybersecurity risk management program (CFR, 2020). The risk management program aims to reduce the likelihood of device functionality being compromised, intentionally or unintentionally, by inadequate cybersecurity. An effective cybersecurity risk management program should address cybersecurity in both the premarket and postmarket medical device development phases.

The literature review indicates that a framework should be easy to understand and easy to use by organisations. To address that, the framework should provide step by step guidance on how to conduct each step of the risk management process. This guidance should greatly assist developers with limited experience in adopting a risk management process. The literature review also identified that a framework needs to produce valid and credible results for organisations that the security personnel will accept.

7.2.2 Objective 2

The evaluation of the WBANSecRM framework is comprised of two distinct stages. Stage 1 involved trialling the WBANSecRM framework in an industrial setting, while stage 2 consisted of validation through expert review.

7.2.2.1 Stage 1 – Industrial Implementation

The process to implement the alpha version of the WBANSecRM framework is outlined in Figure 7-1.

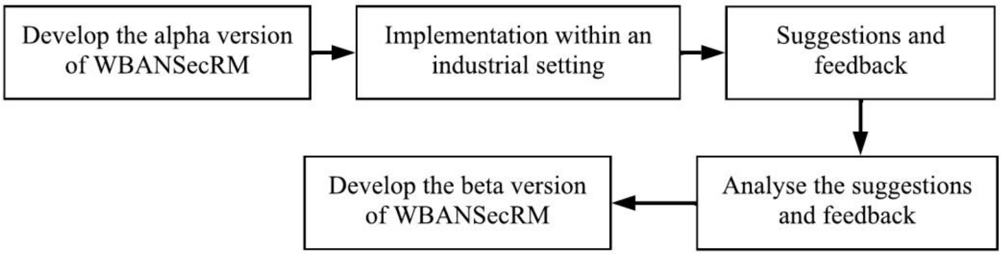

Develop the alpha version of WBANSecRM
Implementation within an industrial setting
Suggestions and feedback
Analyse the suggestions and feedback
Develop the beta version of WBANSecRM

Figure 7-1: Industrial implementation

Implementation: The alpha version of the WBANSecRM framework was implemented in an Irish WBAN development company. After implementation of the WBANSecRM framework, a penetration test was conducted with the help of a third-party penetration service provider to evaluate the efficacy of the implemented controls in mitigating the threats and vulnerabilities. The penetration tests identified two vulnerabilities; 1) potential denial of service points in two API endpoints and 2) security misconfiguration – stack traces enabled. The first vulnerability occurred because input validation of the input data stream was not implemented for those API endpoints. On the other hand, the second vulnerability's root cause was not handling the exception inside the code properly. The developer was advised to add input validation for all API endpoints and write the exception message in the error log file. Writing in the error log file will assist the developer in auditing to identify the root cause of the issue. The developer was also advised to assure all API endpoints reply with a user-friendly error message instead of sending the stack trace. The alpha version of the WBANSecRM framework could not identify these two vulnerabilities as the alpha WBANSecRM framework did not include a unit test step and a code review step during the control implementation phase. Both steps were added in the beta version of the WBANSecRM framework.

Suggestions and Feedback: Upon successfully implementing the alpha version of the WBANSecRM framework, a follow-up semi-structured interview was conducted with the CTO, the development team and a representative of the penetration test service provider. The goal of the interview was to gather suggestions and feedback about the usability and efficacy of the WBANSecRM framework. The representative of the penetration test service provider raised the concern that the alpha version of the WBANSecRM framework did not consist of any code review stage. A code review stage can help to identify coding errors during the implementation phase. The resulting suggestions and feedback from the review session are presented below:

- Identify the threats and vulnerabilities at the requirement analysis phase to produce the security and privacy requirements
- A guideline for the system architecture review would be useful to check whether the minimum security and privacy requirements are taken into consideration
- A risk evaluation process would be helpful to identify the severity level of the threats and vulnerabilities
- A risk treatment process will be useful to identify the risks which require controls to mitigate
- A code review process during the control's implementation will help to minimise coding errors
- Conduct unit testing during the implementation phase to identify whether the control is implemented correctly.

To address the above suggestions, a review of existing risk management frameworks was conducted to explore the steps and processes to manage security and privacy risk while developing applications. The review identified AAMI TIR 57 as a widely used security risk management framework for developing healthcare-based applications. AAMI TIR 57 is also recommended by several standards such as ISO 62304 and regulatory bodies such as the FDA and HIPAA. The review also identified that IEC 80001-5-1 defines the secure lifecycle requirements for developing and maintaining healthcare applications. During the development of the beta version of the WBANSecRM framework, the risk management guidelines provided by AAMI TIR 57 and security activities in the healthcare application lifecycle guidance provided by IEC 80001-5-1 were adopted. Once the beta version of the WBANSecRM framework was developed, the next step (stage 2) was to validate it by expert review.

7.2.2.2 Stage 2 – Validation by Expert Review

The process to validate the WBANSecRM framework by expert review is outlined in Figure 7-2.

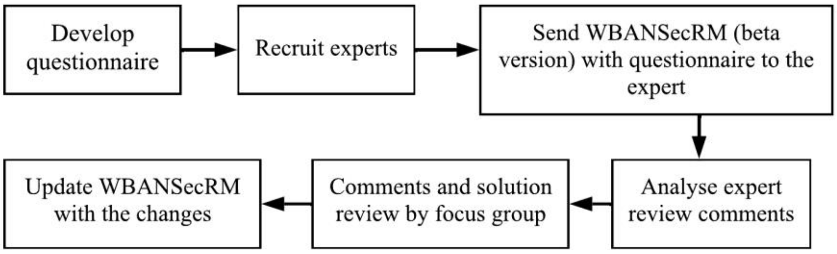

Develop questionnaire
Recruit experts
Send WBANSecRM (beta version) with questionnaire to the expert
Analyse expert review comments
Comments and solution review by focus group
Update WBANSecRM with the changes

Figure 7-2: Validation by expert review

The expert review was completed in six stages. The first stage was to develop the questionnaire, followed by recruiting appropriate experts. Five independent experts were recruited to review the beta version of the WBANSecRM framework. The aim of the expert review was to assess the usability and efficacy of the WBANSecRM framework. The usability of the WBANSecRM framework was assessed based on whether the WBANSecRM framework is easy to use, easy to understand and consists of adequate details for a developer to use. Additionally, the efficacy of the WBANSecRM framework was assessed based on whether the framework consists of the appropriate controls, and whether these controls consist of sufficient implementation detail for developers to implement the controls. The expert review of the WBANSecRM framework returned forty-nine comments which suggested changes to the WBANSecRM framework. After carefully considering the experts' comments, the focus group agreed with thirty-six comments resulting in nineteen amendments to the WBANSecRM framework. Additionally, the focus group also agreed with another seven comments and considered this future research work. Furthermore, there were four comments for which the focus group agreed not to take any further action to address those comments due to them being out of the scope of this research. Finally, two more comments required more clarification from the reviewer. As the reviewer did not respond to the request for clarification, no further action was taken to address those comments. The amendments are summarised in section 6.6 followed by a list of future work presented in section 6.7.

7.2.3 Research Question Revisited

As outlined in the introduction chapter of this thesis, this study aims to investigate *"How can the development of a wireless body area network (WBAN) data security and privacy risk management framework for healthcare applications assist developers and organisations in improving the security and privacy of data, and put them on the road to regulatory compliance?"*

Organisation perspective: The alpha version of the WBANSecRM framework is divided into three stages, namely identification of possible threats and vulnerabilities, implementation of controls, and evaluation of the efficacy of the controls. The framework employs threat modeling to identify threats and vulnerabilities. The control implementation details provided by the framework assist developers in implementing safeguards to mitigate the identified threats and vulnerabilities. During the review of the alpha version of the WBANSecRM framework in an industrial setting, the developer team expressed that the framework was user-friendly and the control implementation details were helpful and easy to use.

The organisation also commented that the alpha version of the WBANSecRM framework assisted the developers in partially overcoming the challenges for assuring security and privacy of WBAN applications. Furthermore, the evaluation of the WBANSecRM framework's efficacy was partly conducted by an independent penetration service provider who commented that "*The targeted platforms were the API that the mobile application interacts with. There were no major issues found, with the two issues being potential Denial of Service targets within the API. It was not possible to access other user's data, or to make the API crash completely. The authentication side of the systems was found to be very secure and it was not possible to tamper with the tokens in any way*". The organisation also suggested that having a risk evaluation process would help identify the severity level of the threats and vulnerabilities. A risk treatment process will also help identify the risks that require mitigation.

Experts' perspective: In addition to the implementation within the industrial setting, the expert review findings also indicate that the WBANSecRM framework will be very useful for developers and organisations to assure security and privacy. In response to the WBANSecRM framework's usability, two experts (1 and 4) think the framework is easy to understand and two experts think it is neither easy nor difficult to follow the framework. Expert 3 commented that *"it feels too academic for a user-friendly tutorial document"*. As the WBANSecRM framework was written as part of this research study, future work is to develop a web application of the WBANSecRM framework to improve usability.

In response to the WBANSecRM frameworks' effectiveness, three experts think the framework will be effective in assuring the security and privacy of the WBAN applications. Four experts out of five think that the WBANSecRM framework has sufficient details for the developer to use with comments such as:

"A very extensive framework, so it should be effective" and *"The framework seems to address all key points that I would expect to be in a security/privacy centered development process"*

Four out of five experts stated that they would consider using this framework if they planned to develop a WBAN based healthcare application.

In response to the WBANSecRM framework's effectiveness, three experts commented that the framework completely ignores the safety and security relationship. In Clause 4.2 of ISO 62304 it is recommended that healthcare software manufacturers should establish safety and security as part of risk management. But AAMI TIR 57 suggests using two separate processes to manage safety risks, and security and privacy risk. As the WBANSecRM framework was developed to assure security and privacy of a WBAN based healthcare application, mitigating safety-related risks is out of the scope of this study. Considering the scope of this research study, the focus group agreed not to take any further action to address this comment.

Expert 2 commented that the WBANSecRM framework does not cover privacy. To cover the privacy issue, the WBANSecRM framework recommends using access control, authentication, annomysation, non-repudiation and authorisation to restrict unauthorised access to data. Additionally, the WBANSecRM framework also suggests using cryptographic controls to encrypt data at rest and while in transit. Expert 3 commented that it feels too academic for a user-friendly tutorial document. Additionally, expert 5 commented that frequent jumps to the appendices and back make it hard to follow. As the WBANSecRM framework document was written as part of a research study, the focus group agreed to create a web version of the WBANSecRM framework as future work. The web version of the WBANSecRM framework will provide easy navigation to the different chapters and appendices of the WBANSecRM framework.

The overall research question states that the WBANSecRM framework should put WBAN developers on the path to regulatory compliance. This means they should comply with the relevant security and privacy standards and risk management frameworks. The WBANSecRM framework has been developed based on recommendations and best practice guidelines provided by regulations such as FDA, HIPPA and GDPR, and by standards such ISO/IEC 80001-2-2, AAMI TIR 57, NIST 800-53 and ISO 27002, which will also help organisations on the path of regulatory compliance. The contributions and impact of this research are discussed in the next section.

7.3 Implications of Findings

7.3.1 Theoretical Implications

Due to the advancement in technology and the increasing popularity of healthcare-based applications, WBAN applications are one of the primary targets for security breaches and cyber threats. In a WBAN application, communication of patient health-related information needs to be private, confidential and unaltered while collecting the data from a sensor or sending it over to the internet to a server. It is also necessary to use an appropriate encryption technique to protect data from being tampered with or leaked. Due to the resource constraints in terms of power, memory and computational capability, the security specifications and solutions proposed for other networks do not apply to WBAN applications. It is necessary to implement controls that guarantee the confidentiality, integrity, availability and privacy of patient health record data in WBAN based healthcare applications. As complex mechanisms require more computation and power resources, it is necessary to have a solution that minimises both.

The literature indicates that most of the security approaches provide for data confidentiality, integrity, authentication, key management and cryptographic techniques. Very few of the approaches address countermeasures for privacy, auditability, trust management, intrusion detection and resilience. As WBAN PHR data can be stored on client’s mobile devices, however none of the existing security approaches provide any guidelines on how to achieve security and privacy for those mobile devices. Additionally, WBAN based healthcare application need to assure data security and privacy by adopting guidelines provided by different regulatory bodies as they process patient PHR data.

Adopting a cybersecurity framework is crucial for organisations to establish a standard for assessing the efficiency of security and privacy controls and ensuring compliance with regulations. However, implementing such a framework can be challenging and requires overcoming various technical and organisational obstacles (Townsend, 2017). According to

Townsend (2017), 95% of organisations have experienced difficulties in implementing their chosen cybersecurity framework due to reasons such as shortage of skilled personnel, inadequate budget, and lack of management support. The literature suggests that small organisations are confronted with significant challenges in complying with regulations related to information security and privacy, primarily due to their limited understanding of the relevant frameworks. As a result, they often fail to conduct proper risk assessments or develop adequate security and privacy policies.

The literature review identified a total of six risk management frameworks: ISO/IEC 80001-1:2010, AAMI TIR57, ISO 14971, ISO 27005, OCTAVE and NIST 800-30. An initial analysis found that only two of these six frameworks were 'healthcare specific' security and privacy risk management frameworks: ISO/IEC 80001-1:2010 and AAMI TIR57. Among them, IEC 80001-1 guides managing risks associated with medical devices when connecting to IT networks. The framework aims to help organisations define the risk management roles, responsibilities, and activities to achieve medical device safety and security. IEC 80001-1:2010 was primarily developed for applications within a healthcare delivery organisation's IT network, whereas WBAN applications may operate in public, open networks using short-range communication media. IEC 80001-1:2010 does not provide any guidelines for assuring security and privacy in resource-constrained sensor devices that communicate over Bluetooth.

7.3.2 Practical Implications

IEC 62304 recommends that organisations establish and maintain a risk management process to manage risk associated with security. The process should provide a methodology to identify the vulnerabilities, evaluate the associated threats, and implement risk controls to mitigate these threats. The literature review indicates that a framework should be easy to understand, easy to use, and easily adaptable by organisations. The framework also needs to produce valid and credible results for the organisations that the security personnel will accept. The risk management framework should use a qualitative and/or quantitative approach for conducting risk assessment.

When it comes to conducting the security risk assessment at both the requirements analysis and system architecture phases, AAMI TIR57 is quite unclear. However, the WBANSecRM framework lays out the necessary steps to perform a comprehensive security risk assessment at both phases, ensuring that the process is thorough and effective. Aditionally, the WBANSecRM framework provides a comprehensive list of assets, threats, and vulnerabilities that are specific to WBAN applications. This list can serve as a starting point for conducting security risk analysis and can be used in conjunction with the steps outlined in the aforementioned framework to ensure a thorough and effective process.

At the system architecture phase, AAMI TIR57 fails to provide any guidelines for conducting design reviews. However, the beta version of the WBANSecRM framework has taken steps to address this issue by including design review guidelines recommended by IEC 80001-5-1. By incorporating these guidelines into the framework, it becomes a more comprehensive and effective tool for conducting security risk assessments in the context of WBAN applications. Additionally, AAMI TIR57 fails to include risk treatment as part of the security and privacy risk assessment process, leaving a significant gap in the framework. However, the beta version of the WBANSecRM framework has addressed this issue by including risk treatment steps as part of the security and privacy risk assessment process. These steps help to identify unacceptable risks that require controls to mitigate and ensure that a comprehensive approach is taken to manage risks in WBAN applications.

In addition to providing risk treatment steps, the beta version of the WBANSecRM framework also includes a mapping of possible threats and vulnerabilities with respective risk controls. This mapping helps to identify the most effective controls for mitigating specific risks and ensures that a targeted approach is taken to managing security and privacy risks in WBAN applications. The framework also includes implementation details for these controls, making it easier for organisations to understand how to implement them effectively. Overall, the beta version of the WBANSecRM framework is a comprehensive tool for managing security and privacy risks in the context of WBAN applications.

7.4 Threats to Validity

The measures taken to address the reliability and validity of this research have been outlined in section 4.10 of chapter 4. This section recaps those measures and addresses additional threats that have arisen.

7.4.1 Reliability

Reliability is concerned with the extent to which the results of a study or a measure are repeatable by a different researcher conducting the same experiment. To safeguard the reliability of this research, the WBANSecRM framework produced in this study was developed based on the guidelines provided by AAMI TIR 57. During the evaluation of the alpha version of the WBANSecRM framework, a penetration test was carried out with the assistance of a third-party penetration service provider. The penetration test did not reveal any major issues, except for two potential Denial of Service targets within the API. The test showed that it was not possible to access other users' data or crash the API entirely. Additionally, the authentication side of the system was found to be highly secure, as it was not possible to tamper with the tokens in any way. Furthermore, this study also documented the comments received during the expert review and how those comments were incorporated into the WBANSecRM framework. To analyse the reviewer comments a protocol was developed based on the guidelines presented by Saunders, Lewis and Thornhill, (2009, pp.478). To assure the reliability of analysing the reviewer comments, a focus group was set up which consisted of two members from the RSRC having extensive expertise in the area of security and privacy for medical devices. The focus group members reviewed each proposition to reach a consensus to address the comments.

7.4.2 Validity

The validity of the research can be defined as the best available approximation to the truth of a given proposition, inference, or conclusion. The validity of this research has been addressed from four different perspectives: conclusion validity, internal validity, construct validity, and external validity.

7.4.2.1 Conclusion Validity

Conclusion validity is the degree to which the conclusions made about a relationship are reasonable, credible and believable. To address conclusion validity, this study took a number of measures which included:

- Production of a protocol to conduct a structured literature review
- Production of a protocol based on the strategy identified by Catherine Dawson (2002, p.69) to design the questionnaires for conducting an expert review
- Production of a protocol to conduct the expert review that ascertained that all the relevant information had been gathered from the expert

7.4.2.2 Internal Validity

Internal Validity is concerned about whether the results reported are, in reality being triggered by researcher interference rather than any other conflicting factor. To address concerns over internal validity, a number of measures were employed which included:

- The organisation selected the period over which the WBANSecRM framework was to be implemented. During the implementation of the WBANSecRM framework, no other changes were made to the development process, which helped assure that any identified effects were due to using the WBANSecRM framework

- Data triangulation uses various data sources, including organisational interviews, and analysing existing documents related to assuring security and privacy for medical devices. Method triangulation was achieved using multiple experts from academia and industry and industrial pilot in a WBAN based application development organisation

7.4.2.3 Construct Validity

Construct validity is concerned with whether the data collection measure measures what it aims to measure. This study employed expert review of the WBANSecRM framework followed by discussion with supervisors about these comments before reaching an agreement for changes to minimise the threats to the construct validity.

7.4.2.4 External Validity

External validity addresses the degree to which the findings of a research study can be generalised in other contexts beyond the context in which it was initially performed. To address concerns over the external validity of this study, the alpha version of the WBANSecRM framework was trialled in an industrial setting, and the beta version of the WBANSecRM framework was further validated by expert review. Despite taking the above measures, a number of threats to the external validity of this research still exist. In relation to generalisability, some authors contend that there are difficulties with generalising qualitative research as *'its statements are often made for a certain context or specific cases'* (Flick, 2014, p.495).

In validating this research, the WBANSecRM framework was implemented in one organisation which raises questions about the generalisability of the WBANSecRM framework for all WBAN application development organisations. Although the development of the WBANSecRM framework was based on widely recognised standards and methods, has undergone international expert review, and has been published in international conferences and journals, implementation in a larger number of organisations is required to strengthen generalisability. Implementation of the WBANSecRM framework within more than one organisation was deemed impractical for this study due to resource constraints.

A further threat to validity arises because the expert evaluation of the WBANSecRM framework involved responding to questions that required a '*Likert scale*' type response. Responses to questions of this type can be subjective as, for example, one expert's understanding of the difference between '*easy*' and '*very easy*' may differ from another expert. While threats of this nature will always exist with responses of this type, it is partially addressed by each question of this type having a follow-up question of *'Please state why as a rationale for your opinion.'* This threat may have been further reduced by interviewing a larger number of experts. However, this was not deemed practical due to time constraints to source a large number of experts having expertise in assuring security and privacy.

A final threat to the validity of the results is related to the security and privacy requirements and their respective control implementation details. A number of medical device standards and guidelines were used to identify the security and privacy requirements and to develop their respective implementation details. As these standards and guidelines are not static documents and are amended from time to time, so amendments may result in a change to security and privacy requirements as well as the respective control implementation details. Therefore, any change in the standards and guidelines may necessitate a corresponding change to the WBANSecRM framework. The methodology and sources used to identify the controls with respective implementation details will assist with future amendments to the WBANSecRM framework.

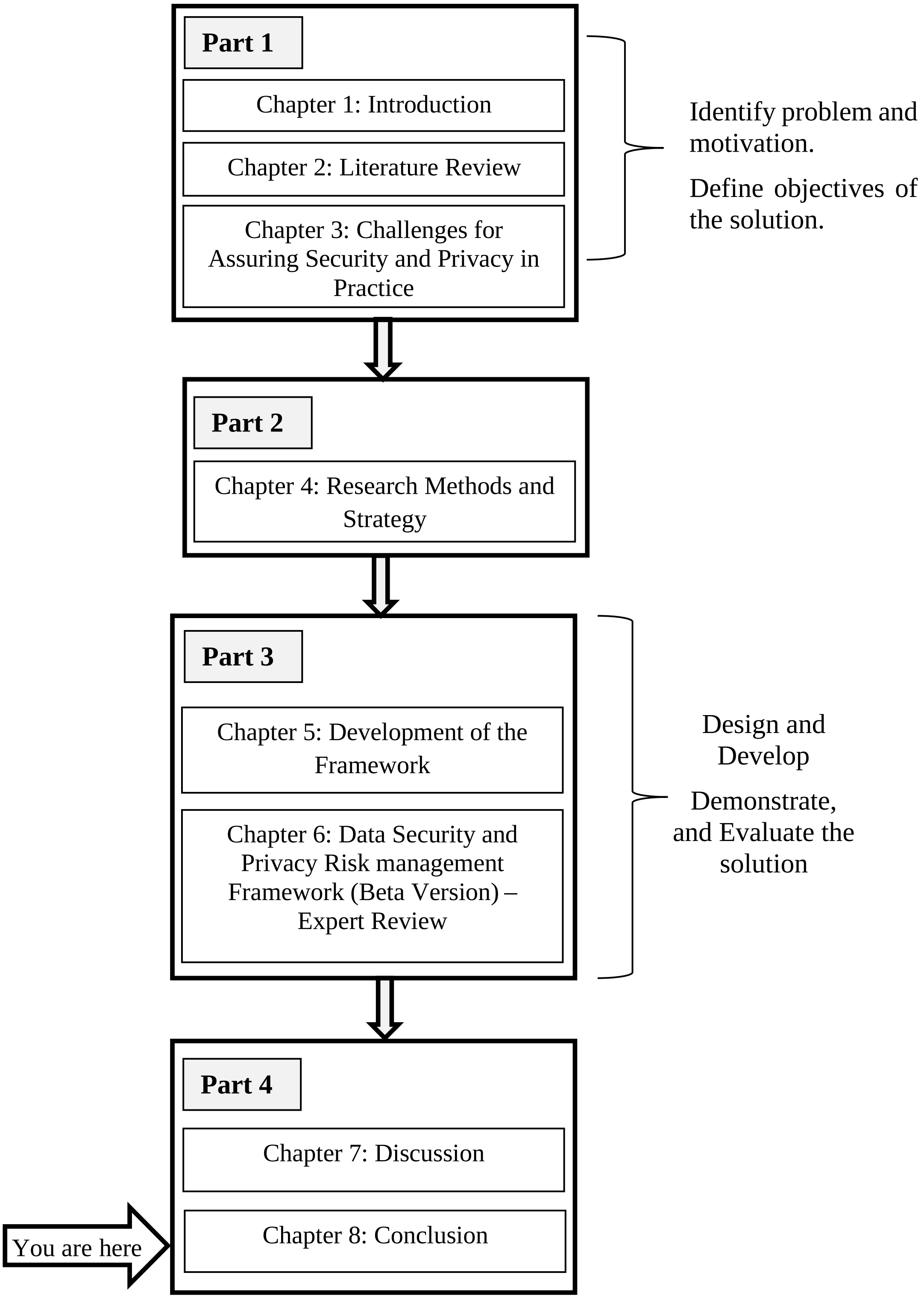
7.5 Summary

Through a thorough literature review and interviews with a WBAN application development organization, it became evident that developers encounter a range of difficulties when it comes to ensuring the security and privacy of WBAN applications. In response to these challenges, this research project has developed the WBANSecRM framework. The primary objective of this framework is to provide practical assistance to developers in enhancing the security and privacy aspects of WBAN applications. The literature review suggests that a framework should aim to be simple and user-friendly for organisations. In order to achieve this, the framework should offer clear and concise instructions for each step of the risk management process. This will be particularly helpful for developers who may have limited experience with risk management processes. Additionally, the literature review highlights the importance of a framework generating reliable and trustworthy results that security personnel will find acceptable.

The WBANSecRM framework comprises a comprehensive list of assets, threats, vulnerabilities, and controls that are uniquely tailored to WBAN applications. The framework's implementation details are designed to be easily understood even by those with minimal security expertise, thereby reducing development time and cost. In addition, the framework is designed to identify the security and privacy requirements that need to be taken into consideration during the development of a WBAN application's architecture. By doing so, it will assist organisations in gaining a complete understanding of the WBAN architecture and its security and privacy considerations. The WBANSecRM framework not only lists assets, threats, vulnerabilities, and controls specific to WBAN applications but also provides step-by-step guidance on how to conduct each stage of the risk management process. This guidance will be particularly useful for developers who may have limited experience in implementing a risk management process. Apart from its implementation in industrial settings, the expert review findings suggest that the WBANSecRM framework will be highly valuable in assuring security and privacy for developers and organizations alike. In terms of the framework's usability, two experts have expressed that it is easy to comprehend.

The next chapter examines the research contribution and outline the potential areas for future research.

Map of Thesis


Part 1
Chapter 1: Introduction
Chapter 2: Literature Review
Chapter 3: Challenges for Assuring Security and Privacy in Practice
Identify problem and motivation.
Define objectives of the solution.
Part 2
Chapter 4: Research Methods and Strategy
Part 3
Chapter 5: Development of the Framework
Chapter 6: Data Security and Privacy Risk management Framework (Beta Version) – Expert Review
Design and Develop
Demonstrate, and Evaluate the solution
Part 4
Chapter 7: Discussion
Chapter 8: Conclusion
You are here

8 Conclusion

8.1 Introduction

This final chapter summarises the findings of this study followed by the contribution of this research to the body of knowledge is presented along with the impact of the research. Finally, the limitations of this research are discussed before the potential for future research is considered.

8.2 Summary

The main design requirements for any WBAN application is that the body sensor node needs to be extremely small and thin, capable of wireless communication, and use minimal power for data collection and processing (Antonescu and Basagni, 2013). User requirements such as privacy, safety, ease of use, security and compatibility are also of great importance (Salayma et al., 2017). WBAN applications operate in an environment where many people have open internet access, and thus WBAN applications are vulnerable and open to many types of attacks and threats. A security breach in a WBAN based healthcare application not only costs money; in some cases, it can create a life-threatening event. So, security and privacy safeguards need to be considered during the development of this type of healthcare application. A literature review, conducted as part of this study, indicated that WBAN applications can be affected by a total of eleven types of attack. Among them, denial-of-service, eavesdropping, replay attacks, and data modification attacks are common attacks on WBAN applications. Additionally, the literature review also indicates that there are a total of twenty-two requirements that need to be considered for assuring the security and privacy of WBAN applications.

A review of existing risk management frameworks was conducted in order to understand how any of these frameworks could contribute to the development of a WBAN risk management framework. This review identified the following six risk management frameworks: ISO/IEC 80001-1:2010, AAMI TIR57, ISO 14971, ISO 27005, OCTAVE and NIST 800-30. An initial analysis found that only two of these six frameworks were ‘healthcare specific’ security and privacy risk management frameworks: ISO/IEC 80001-1:2010 and AAMI TIR57. IEC 80001-1 guides managing risks associated with medical devices when connecting to IT networks. IEC 80001-1:2010 was primarily developed for applications within a healthcare delivery organisation’s IT network, whereas WBAN applications may operate in public, open networks using short-range communication media. AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices. A WBAN application consists of resource-constrained sensor devices with limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications. AAMI TIR57 does not provide any guidance for managing security and privacy risks for resource-constrained sensor devices.

Considering the challenges that organisations and developers face for assuring security and privacy of PHR data, the WBANSecRM framework has been developed as part of this study. The aims of the WBANSecRM framework are that:

- It should provide a clear pathway for developers to assure data security and privacy, and assist them to fulfil the medical device security and privacy related regulations
- It should assist medical device development organisations who have limited resources and expertise in this area to assure security and privacy

The literature review indicates that a framework should be easy to understand and easy to use by organisations. The framework also needs to produce valid and credible results for the organisation. The risk management framework should use a qualitative and/or quantitative approach for conducting risk assessment. Furthermore, the framework should also consist of the following phases to assure security and privacy:

- Identification of assets
- Identification of threats and vulnerabilities

- Risk evaluation
- Risk treatment
- Risk acceptance
- Selection of security and privacy risk controls
- Develop the implementation details for security and privacy risk controls
- Implement the selected security and privacy risk controls
- Monitoring the effectiveness of the security and privacy risk controls

The WBANSecRM framework consists of three key elements – a risk assessment process to identify and evaluate the threats and vulnerabilities, a list of WBAN security and privacy controls with implementation details, and a process to evaluate the effectiveness and efficacy of the controls. This framework provides a list of assets, threats and vulnerabilities which are specific to WBAN applications. The list of assets, threats and vulnerabilities will assist WBAN development organisations in conducting the risk assessment.

The WBANSecRM framework was developed in two stages. The alpha version of the WBANSecRM framework was developed, consisting of the security and privacy requirements with respective countermeasures required to assure the security and privacy of WBAN based healthcare applications. Upon completion of the development of the alpha version of the WBANSecRM framework, it was then implemented in an industrial setting. The feedback and comments received from the industrial trial were analysed, which resulted in the beta version of the WBANSecRM framework. To evaluate the usability and efficacy of the beta version of the WBANSecRM framework, an expert review was conducted with a combination of experts from both academia and industry. On return of the completed questionnaire, the comments received from the experts were analysed. Once this analysis was complete, the comments and proposed changes to address the respective comments were reviewed by a focus group. The focus group reviewed the experts' comments and the suggested changes, and through discussion a consensus was reached on which changes should be made to the WBANSecRM framework.

8.3 Research Contribution

Through the literature review and interview with a WBAN application development organisation, this research identified the challenges faced by developers to assure security and privacy of WBAN applications. The WBANSecRM framework aims to assist developers in overcoming the challenges to assure security and privacy. The final activity of the Action Design Research process (Chapter 4, section 4.9) is to communicate the problem and its importance, the artefact, its utility and novelty, the rigor of its design and its effectiveness. This communication has been achieved through the publication of research articles in international conference proceedings and international journals. This research has provided contribution at a number of levels:

- Contribution of knowledge to WBAN application security and privacy research community
- Contribution of knowledge to WBAN application development community
- Contribution of knowledge to the security and privacy risk management community

8.3.1 Contribution of Knowledge to WBAN Application Security and Privacy Research Community

To develop an effective solution for assuring security and privacy, it is necessary to explore the attacks landscape and security and privacy requirements of WBAN applications. Unfortunately, there was no comprehensive list of attacks and security and privacy requirements available for WBAN applications. Therefore, a structured literature review was conducted to identify the potential attacks and security and privacy requirements for assuring security and privacy in WBAN applications (Paul *et al.*, 2019). The WBANSecRM framework will contribute the following to the security and privacy research community:

- The literature review indicates that a WBAN application can be affected by a total of eleven types of attack. Among them, denial-of-service, eavesdropping, replay attacks, and data modification attacks are common attacks for a WBAN application.
- The literature review also revealed that there are twenty-two requirements to assure the security and privacy of WBAN applications. Among them data confidentiality, integrity and availability, are the most common requirements to assure the security and privacy of WBAN applications.
- Existing solution approaches only address issues related to data confidentiality, integrity, authentication, key management and cryptographic techniques. Very few of the approaches address countermeasures for privacy, auditability, trust management, intrusion detection and resilience.
- WBAN PHR data can be stored on client's mobile devices. None of the existing security and privacy approaches provide any guidelines on how to achieve security and privacy for those mobile devices.

8.3.2 Contribution of Knowledge to WBAN Application Development Community

This research developed a data security and privacy risk management framework for WBAN based healthcare applications (Paul *et al.*, 2021). The WBANSecRM framework will provide the following benefits to organisations:

- The WBANSecRM framework consists of a list of assets, threats, vulnerabilities, and controls with implementation details specific to WBAN applications. This list will assist the developer in getting an understanding of the threat and vulnerability landscape of WBAN applications
- The WBANSecRM framework provides detailed guidance on how to conduct each step of the risk management process. This guidance should greatly assist developers with limited experience in implementing a risk management process

- The WBANSecRM framework is developed based on the recommendations and best practice guidelines provided by regulations such as FDA, HIPPA and GDPR, and by standards such ISO/IEC 80001-2-2, TIR 57, NIST 800-53 and ISO 27002, which will help to put the organisation on the road to regulatory compliance
- The WBANSecRM framework guides risk assessment at both the requirements analysis and the system architecture phases. This guidance will help the organisation understand how data flows around the system and assist them in identifying the assets that need protection
- The WBANSecRM framework provides appropriate security and privacy controls, along with their implementation details, for a WBAN application. The implementation details will assist developers in implementing the security and privacy controls

8.3.3 Contribution of Knowledge to the Security and Privacy Risk Management Community

ISO 62304 is a widely known standard which provides guidelines for developing healthcare applications. ISO 62304 states that organisations need to implement a risk management process while developing healthcare software to assure security and privacy. To achieve this, AAMI TIR57 is a widely used risk management framework which guides the developer to perform information security and privacy risk management to address security and privacy risks within medical devices. WBAN applications consist of resource constrained sensor devices which have limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications. This research developed the WBANSecRM framework by adopting guidelines provided by AAMI TIR 57 (Paul *et al.,* 2021). The WBANSecRM framework will contribute the following to the security and privacy risk management community:

- AMI TIR57 does not clearly define how to conduct the security and privacy risk assessment at both the requirements analysis and the system architecture phases. Based on the recommendation of ISO 62304 Clause 5.2 and 5.3, this framework conducts risk assessment at the requirements analysis and system architecture phase of the development lifecycle. The WBANSecRM framework provides the steps to conduct security and privacy risk assessment at both phases. The security and privacy risk assessment helps to identify, analyse and evaluate potential security and privacy risks. This assessment helps an organisation to make decisions about which risks require controls

- The WBANSecRM framework provides a list of assets, threats and vulnerabilities which are specific to WBAN applications, which can be used as a starting point for conducting risk analysis

8.3.4 Lessons Learned as a Result of this Research

In addition to the above contributions, a number of lessons have been learnt by performing this research. These lessons are:

- Identifying the threats and vulnerabilities step in the alpha version of the WBANSecRM framework requires threat modelling. During the pilot implementation in the organisation, I assumed that organisations would have resources with knowledge of threat modelling. But during the implementation, I found out that there was no resource available who had experience conducting threat modelling. So, the lesson learned was never to assume that developer will have expertise in threat modelling.
- While evaluating the controls' effectiveness after implementing the alpha version of the WBANSecRM framework, the penetration test discovered that the stack traces were enabled for some of the API endpoints. Discussion with the organisation revealed that the developers did not use a code review process during product development. So, the lesson learned was never to assume that all organisations will have a code review policy or code will be reviewed by another developer.

8.4 Future Research

As a number of limitations were identified in the previous chapter, further research is required to address those limitations. To address the generalizability concern, the WBANSecRM framework could be implemented in a large number of organisations. Implementing the WBANSecRM framework in a large number of organisations will offer the developer perspectives on the usefulness and usability of the WBANSecRM framework and thus further opportunity to amend and improve it.

As stated earlier, assuring security and privacy is a key requirement from the various medical device regulations and legislation. In addition to that, regulations and legislation are also implemented to assure the safety of the product. The WBANSecRM framework suggests using the guidelines provided by ISO 14971 in parallel to mitigate the safety-related risk. Conducting safety risk management alongside the WBANSecRM framework might be a resource constraint for a small and medium-sized organisation. To address this issue, further research can be done to combine both processes and develop a common framework that will assist organisations in assuring security and privacy and mitigating the safety risk.

The WBANSecRM framework developed as part of this research consists of a manual process to identify the possible threats and vulnerabilities from various databases. As the threat and vulnerability landscape is frequently changing and new threats and vulnerabilities are emerging every day, carrying out this manual process will require extensive time and human effort. Further research can be done to address this issue to convert the current framework into a web tool and add machine learning techniques to automatically assure that the threats and vulnerabilities database is up-to-date. Furthermore, developing the threat description for each asset and sub-asset will help developers to understand how the asset and sub-asset will be affected if the attacker launches an attack.

Finally, consider adding formal verification process to provide a systematic approach for identifying the flaws of a protocol. Also develop worked examples or code snippets for each risk control which will assist the developer during the implementation of the risk control. In addition to that, developing a web version of the WBANSecRM framework may also increase usability and make it more user-friendly to developers and organisations.

8.5 Conclusion

Assuring security and privacy of data is a key concern and is a challenging task faced by developers of WBAN applications. Developers have difficulties in assuring security and privacy of WBAN based healthcare applications for a number of reasons which include: lack of knowledge about market-specific regulatory requirements and security and privacy standards; lack of understanding of what assets need to be protected in WBAN ecosystems; and difficulty with the identification of appropriate security controls and lack of security control implementation details. A literature review was conducted to present a holistic view of attack types and security and privacy requirements related to WBAN applications. The literature review indicates that WBAN applications are vulnerable to 11 attack types with DoS, eavesdropping and replay attacks being the most common. In addition, there are 22 security and privacy requirements related to WBAN, with data confidentiality, integrity, privacy, fine-grained access control, lightweight cryptography algorithms and key management being the most referenced. The reviewed literature also indicated that none of the existing security approaches provide countermeasures for all of the identified attacks and security and privacy requirements, although most of the approaches provide for data confidentiality, integrity, authentication, key management, and cryptographic techniques. However, very few of the approaches address countermeasures for auditability, trust management, intrusion detection and resilience.

In this research, six existing risk management frameworks were reviewed to identify which of them are designed specifically for developing healthcare-based applications. The review indicates that only two of these six frameworks were 'healthcare specific' for assuring security and privacy, that is ISO/IEC 80001-1:2010 and AAMI TIR57. IEC 80001-1:2010 was primarily developed for applications which operate within a healthcare delivery organisation's IT-network, whereas WBAN applications may operate in a public, open networks using short-range communication media. Therefore, TIR 57 was considered more suitable for this research as TIR 57 provides guidance for manufacturers to perform information security and privacy risk management to address security and privacy risks during the development of medical devices. However, both TIR 57 and ISO/IEC 80001-1 lack a process for selecting security controls, lack security control implementation details, and they do not provide any guidance to assure security and privacy for resource constrained sensor devices. Therefore, a new data security and privacy risk framework is needed to assure the security and privacy of WBAN data.

The WBANSecRM framework developed as part of this research addresses the challenges detailed above. The WBANSecRM framework was developed in three stages, the alpha, beta and gamma versions. Once the alpha version of the WBANSecRM framework was developed, it was implemented within a WBAN development organisation. The developers used the implementation details of the respective controls provided by the alpha version of the WBANSecRM framework to mitigate risk. After the implementation, an external penetration tester was onboarded to evaluate whether the implemented controls were assuring the security and privacy of the application. Upon successfully implementing the alpha version of the WBANSecRM framework in an industrial setting, a follow-up interview was conducted with the CTO and the development team of the organisation. The goal of the interview was to gather suggestions and feedback about the usability and efficacy of the WBANSecRM framework.

The feedback received after the alpha version's industrial trial resulted in the beta version of the WBANSecRM framework.

To address the suggestions received from the organisation, a review of existing risk management frameworks was conducted to explore the steps and processes to manage security and privacy risk while developing applications. The AAMI TIR 57 is a widely used risk management framework for developing healthcare-based applications. This framework is also recommended by several standards such as ISO 62304 and regulatory bodies such as the FDA. During the development of the beta version, the risk management guidelines provided by AAMI TIR 57 were adopted. Furthermore, security activities in the healthcare application lifecycle guidance provided by IEC 80001-5-1 were also taken into consideration. Upon completing the development of the beta version of the WBANSecRM framework, the framework was further validated by expert review. A questionnaire and a beta version of the WBANSecRM framework were presented to five experts for review. After receiving the completed questionnaires, the comments received from the experts were analysed by the author of this study which resulted in a total of 49 comments. Once the analysis was complete, the comments and proposition to address the respective comment were reviewed by a focus group. The focus group reviewed the experts' comments and the suggested changes, and through discussion, a consensus was reached on which changes should be adopted. Finally, a total of nineteen changes to the WBANSecRM framework were agreed upon by the focus group and four changes were considered as future work of the study.

To address the reliability and validity of this research, several measures were taken into consideration. To safeguard the reliability of this research, the WBANSecRM framework was developed based on the guidelines provided by AAMI TIR 57, which is a widely used medical device security risk management framework. To address conclusion validity, this research study produced multiple protocols to conduct a structured literature review, to design the questionnaires for conducting an expert review and a protocol to conduct the expert review.

Furthermore, to address internal validity, no other changes were made to the development process during the implementation of the WBANSecRM framework. This helped assure that any identified effects were due to using the WBANSecRM framework. However, the generalisability of the WBANSecRM framework for all WBAN application development organisations is a concern as the WBANSecRM framework was only piloted in one organisation. To strengthen claims of generalisability, the WBANSecRM framework will need to be implemented in a larger number of organisations. Implementation of the WBANSecRM framework within more than one organisation was deemed impractical for this study due to resource constraints. To partly address this concern, the WBANSecRM framework was reviewed by internationally recognised experts and published in international conferences and journals.

9 References

6749, R. (no date) *RFC 6749 - The OAuth 2.0 Authorization Framework*. Available at: https://tools.ietf.org/html/rfc6749 (Accessed: 22 October 2019).

A. Z. Alshamsi and E. S. Barka (2017) 'Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks', *2017 International Conference on Informatics, Health & Technology (ICIHT)*, pp. 1–7.

AAMI TIR57 (2016) *Principles for medical device security—Risk management*.

Abdullah, A.H. *et al.* (2018) 'Securing Data Communication in Wireless Body Area Networks Using Digital Signatures', *Technical Journal*, 23(02), pp. 50–55. Available at: http://tj.uettaxila.edu.pk/index.php/technical-journal/article/view/757.

Abraham, C., Chatterjee, D. and Sims, R.R. (2019) 'Muddling through cybersecurity: Insights from the U.S. healthcare industry', *Business Horizons*, 62(4), pp. 539–548. Available at: https://doi.org/https://doi.org/10.1016/j.bushor.2019.03.010.

Aceto, G., Persico, V. and Pescapé, A. (2018a) 'The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges', *Journal of Network and Computer Applications*, 107, pp. 125–154. Available at: https://doi.org/https://doi.org/10.1016/j.jnca.2018.02.008.

Aceto, G., Persico, V. and Pescapé, A. (2018b) 'The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges', *Journal of Network and Computer Applications*, 107(July 2017), pp. 125–154. Available at: https://doi.org/10.1016/j.jnca.2018.02.008.

Aileni, R.M. *et al.* (2020) 'Data privacy and security for IoMWT (internet of medical wearable things) cloud', in *IoT and ICT for Healthcare Applications*. Springer, pp. 191–215.

Al-Janabi, S. *et al.* (2017) 'Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications', *Egyptian Informatics Journal*, 18(2), pp. 113–122. Available at: https://doi.org/10.1016/j.eij.2016.11.001.

Al-Janabi, S., Dawood, A. and Salman, A. (2013) 'Distributed Data Security and Privacy in WBAN-Related e-Health Systems', *AL-Mansour Journal*, (20), pp. 121–132.

Al-saleem, S.M., Ali, A. and Khan, N. (2017) 'Energy efficient key agreement scheme for ubiquitous and continuous remote healthcare systems using data mining technique', *Cluster Computing* [Preprint]. Available at: https://doi.org/10.1007/s10586-017-0903-7.

Alberts, C. *et al.* (2003) *Introduction to the OCTAVE Approach*.

Alemdar, H. and Ersoy, C. (2010) 'Wireless sensor networks for healthcare: A survey', *Computer Networks*, 54(15), pp. 2688–2710. Available at: https://doi.org/https://doi.org/10.1016/j.comnet.2010.05.003.

Aljohani, M. and Blustein, J. (2018) 'A study using the in-depth interview approach to understand current practices in the management of personal health information and privacy compliance', *Proceedings - 2018 IEEE International Conference on Healthcare Informatics, ICHI 2018*, pp. 75–86. Available at: https://doi.org/10.1109/ICHI.2018.00016.

Al Alkeem, E., Yeun, C.Y. and Zemerly, M.J. (2016) 'Security and privacy framework for ubiquitous healthcare IoT devices', in *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp. 70–75. Available at: https://doi.org/10.1109/ICITST.2015.7412059.

Alsadhan, A. and Khan, N. (2013) ‘An LBP based key management for secure wireless body area network (WBAN)’, *2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 85–88. Available at: https://doi.org/10.1109/SNPD.2013.32.

Alshamsi, A.Z., Barka, E.S. and Serhani, M.A. (2016) ‘Lightweight encryption algorithm in wireless body area network for e-health monitoring’, in *2016 12th International Conference on Innovations in Information Technology (IIT)*, pp. 1–7. Available at: https://doi.org/10.1109/INNOVATIONS.2016.7880042.

Altaf, F. *et al.* (2019) ‘Privacy preserving lightweight searchable encryption for cloud assisted e-health system’, *2019 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2019*, pp. 310–314. Available at: https://doi.org/10.1109/WiSPNET45539.2019.9032730.

Aman, A.H.M. *et al.* (2021) ‘IoMT amid COVID-19 pandemic: Application, architecture, technology, and security’, *Journal of Network and Computer Applications*, 174, p. 102886.

Ameen, M. Al and Liu, J. (2012) ‘Security and privacy issues in wireless sensor networks for healthcare applications’, *Journal of medical systems*, pp. 93–101. Available at: https://doi.org/10.1007/s10916-010-9449-4.

Amini, S. *et al.* (2011) ‘Toward a security model for a body sensor platform’, *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, pp. 143–144. Available at: https://doi.org/10.1109/ICCE.2011.5722507.

Anand, S. (2011) ‘Security architecture for at-home medical care using body sensor network’, *Int. J. Ad-hoc, Sensor, Ubiquitous Comput*, 2(1), pp. 60–69.

Andrew, A. *et al.* (2018) ‘Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network’.

Anguraj, D.K. and Smys, S. (2019) ‘Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks’, *Wireless Personal Communications*, 104(1), pp. 1–20. Available at: https://doi.org/10.1007/s11277-018-6005-x.

Ankaralı, Z.E. *et al.* (2014) ‘A comparative review on the wireless implantable medical devices privacy and security’, *4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)*, pp. 246–249. Available at: https://doi.org/10.4108/icst.mobihealth.2014.257411.

Antonescu, B. and Basagni, S. (2013) ‘Wireless body area networks: challenges, trends and emerging technologies’, in *8th int. conf. on body area networks*, pp. 1–7.

Ara, A. *et al.* (2017) ‘A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems’, *IEEE Access*, 5, pp. 12601–12617. Available at: https://doi.org/10.1109/ACCESS.2017.2716439.

Arefin, T., Ali, M.H. and Haque, A.K.M.F. (2017) ‘Wireless Body Area Network : An Overview and Various Applications’, pp. 53–64. Available at: https://doi.org/10.4236/jcc.2017.57006.

Arfaoui, A. *et al.* (2019) ‘Context-aware access control and anonymous authentication in WBAN’, *Computers and Security* [Preprint], (xxxx). Available at: https://doi.org/10.1016/j.cose.2019.03.017.

Arya, K. V and Gore, R. (2020) ‘Data security for WBAN in e-health IoT applications’, in *Intelligent data security solutions for e-health applications*. Elsevier, pp. 205–218.

Asam, M. *et al.* (2019) 'Security Issues in WBANs', *arXiv preprint arXiv:1911.04330* [Preprint].

B, M.R.A. and Tandjaoui, D. (2014) 'A Cooperative End to End Key Management Scheme for E-health Applications in the Context', in *ADHOC-NOW Workshops*, pp. 35–46. Available at: https://doi.org/10.1007/978-3-662-46338-3.

Baba, E., Jilbab, A. and Hammouch, A. (2018) 'A health remote monitoring application based on wireless body area networks', *2018 International Conference on Intelligent Systems and Computer Vision, ISCV 2018*, 2018-May, pp. 1–4. Available at: https://doi.org/10.1109/ISACV.2018.8354042.

Bahena, K. and Tu, M. (2016) 'WBAN Security Management in Healthcare Enterprise Environments', *Annual ADFSL Conference on Digital Forensics, Security and Law* [Preprint], (4).

Barakah, D.M. and Ammad-Uddin, M. (2012) 'A survey of challenges and applications of wireless Body Area Network (WBAN) and role of a virtual doctor server in existing architecture', *Proceedings - 3rd International Conference on Intelligent Systems Modelling and Simulation, ISMS 2012*, pp. 214–219. Available at: https://doi.org/10.1109/ISMS.2012.108.

Barker, E., Chen, L. and Moody, D. (2014) 'NIST Special Publication 800-56B Revision 1 Recommendation for Pair-Wise Key- Establishment Schemes Using Integer Factorization Cryptography'. Available at: https://doi.org/10.6028/NIST.SP.800-56Br1.

Barker, E.B. (2016) 'Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms'. Available at: https://doi.org/10.6028/NIST.SP.800-175B.

Baskerville, R.L. (1999) 'Investigating information systems with action research', *Communications of the association for information systems*, 2(1), p. 19.

Bedi, P. *et al.* (2013) 'Threat-oriented security framework in risk management using multiagent system', *Software: Practice and Experience*, 43(9), pp. 1013–1038. Available at: https://doi.org/https://doi.org/10.1002/spe.2133.

Bejtlich, R. (2013) *The practice of network security monitoring: understanding incident detection and response*. No Starch Press.

Benz, M. and Chatterjee, D. (2020) 'Calculated risk? A cybersecurity evaluation tool for SMEs', *Business Horizons*, 63(4), pp. 531–540. Available at: https://doi.org/https://doi.org/10.1016/j.bushor.2020.03.010.

Bharathi, K.R.S. and Venkateswari, R. (2018) 'Security Challenges and Solutions for Wireless Body Area Networks', in *Comp., Comm.. and Signal Proc.* Springer Singapore. Available at: https://doi.org/10.1007/978-981-13-1513-8_29.

Bhattacharya, T. *et al.* (2016) 'Posture detection using WBAN and its application in remote healthcare monitoring', *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, pp. 2027–2034. Available at: https://doi.org/10.1109/WiSPNET.2016.7566498.

Blasco, J. *et al.* (2019) 'Wearables security and privacy', in *Mission-Oriented Sensor Networks and Systems: Art and Science*. Springer, pp. 351–380.

Bouazizi, A. *et al.* (2017) 'Wireless body area network for e-health applications: Overview', in *Int. Conf. on SM2C*, pp. 17–19.

Boulemtafes, A. and Badache, N. (2016) 'Wearable Health Monitoring Systems: An Overview of Design Research Areas', 20, pp. 17–27. Available at: https://doi.org/10.1007/978-3-319-23341-3.

Bowen, G.A. (2009) 'Document analysis as a qualitative research method', *Qualitative research journal* [Preprint].

Bradai, N., Chaari, L. and Kamoun, L. (2011) 'A Comprehensive Overview of Wireless Body Area Networks (WBAN)', *International Journal of E-Health and Medical Communications*, 2(3), pp. 1–30. Available at: https://doi.org/10.4018/jehmc.2011070101.

Braun, V. and Clarke, V. (2013) *Successful qualitative research: A practical guide for beginners*. sage.

BSI (2009) 'BS EN ISO 14971 : 2009 BSI British Standards Medical devices — Application of risk management to medical devices'.

Cagalaban, G. *et al.* (2012) 'A Multilevel Security Framework for Cloud-Based Ubiquitous Healthcare Application Service', in T. Kim et al. (eds) *Computer Applications for Security, Control and System Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 168–175.

Cavallari, R. *et al.* (2014) 'A survey on wireless body area networks: Technologies and design challenges', *IEEE Communications Surveys & Tutorials*, PP(99), pp. 1–23. Available at: https://doi.org/10.1109/SURV.2014.012214.00007.

Cavoukian, A., Taylor, S. and Abrams, M.E. (2010) 'Privacy by Design: essential for organizational accountability and strong business practices', *Identity in the Information Society*, 3, pp. 405–413.

CFR (2020) *Electronic Code of Federal Regulations*. Available at: https://www.ecfr.gov/cgi-bin/text-idx?SID=ba90ee4a08a5ba017a34366276d68234&mc=true&tpl=/ecfrbrowse/Title21/21cfrv8_02.tpl#0 (Accessed: 13 October 2020).

Chakraborty, S. (2018) 'Wireless Body Area Sensor Network in Healthcare Applications', in *SoutheastCon 2018*, pp. 1–2. Available at: https://doi.org/10.1109/SECON.2018.8479124.

Challa, S. *et al.* (2018) 'Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions', *IEEE Consumer Electronics Magazine*, 7(1), pp. 57–65. Available at: https://doi.org/10.1109/MCE.2017.2720193.

Chatterjee, K. (2020) 'An improved authentication protocol for wireless body sensor networks applied in healthcare applications', *Wireless Personal Communications*, 111(4), pp. 2605–2623.

Chen, H. *et al.* (2020) 'Security design of ECG telemonitoring systems', *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020*, pp. 707–711. Available at: https://doi.org/10.1109/ICCEA50009.2020.00154.

Chen, J.Q. and Benusa, A. (2017) 'HIPAA security compliance challenges: The case for small healthcare providers', *International Journal of Healthcare Management*, 10(2), pp. 135–146. Available at: https://doi.org/10.1080/20479700.2016.1270875.

Chen, Q., Lambright, J. and Abdelwahed, S. (2016) 'Towards Autonomic Security Management of Healthcare Information Systems', *Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016*, pp. 113–118. Available at: https://doi.org/10.1109/CHASE.2016.58.

Chin, C.A. *et al.* (2012) 'Advances and challenges of wireless body area networks for healthcare applications', *2012 International Conference on Computing, Networking and*

Communications, ICNC'12, pp. 99–103. Available at: https://doi.org/10.1109/ICCNC.2012.6167576.

Choi, J.M., Kang, H.J. and Choi, Y.S. (2008) 'A study on the wireless body area network applications and channel models', *Proceedings of the 2008 2nd International Conference on Future Generation Communication and Networking, FGCN 2008,* 2, pp. 263–266. Available at: https://doi.org/10.1109/FGCN.2008.216.

Chowdhury, F.S. *et al.* (2018) 'An implementation of a lightweight end-to-end secured communication system for patient monitoring system', *2018 Emerging Trends in Electronic Devices and Computational Techniques, EDCT 2018,* pp. 1–5. Available at: https://doi.org/10.1109/EDCT.2018.8405076.

Chukwunonyerem, J., Aibinu, A.M. and Onwuka, E.N. (2014) 'Review on security of wireless body area sensor network', in *11th Int. Conf. on Elect., Comp. and Computation (ICECCO),* pp. 1–10. Available at: https://doi.org/10.1109/ICECCO.2014.6997583.

Cole, R. *et al.* (2005) 'Being proactive: where action research meets design research', *ICIS 2005 Proceedings,* p. 27.

Creswell, J.W. and Creswell, J.D. (2018) *Research design: qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.

V. Crosby, G. (2012) 'Wireless Body Area Networks for Healthcare: A Survey', *International Journal of Ad hoc, Sensor & Ubiquitous Computing,* 3(3), pp. 1–26. Available at: https://doi.org/10.5121/ijasuc.2012.3301.

Crotty, M. (1998) *The foundations of social research: Meaning and perspective in the research process*. Sage.

Cunningham, J.B. (1993) *Action Research and Organizational Development*. Praeger. Available at: https://books.google.ie/books?id=QOlJunN1TToC.

Darwish, A. and Hassanien, A.E. (2011) 'Wearable and implantable wireless sensor network solutions for healthcare monitoring', *Sensors,* 11(6), pp. 5561–5595. Available at: https://doi.org/10.3390/s110605561.

Das, A.K. *et al.* (2017) 'Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment', *IEEE Journal of Biomedical and Health Informatics,* 22(4), pp. 1310–1322. Available at: https://doi.org/10.1109/JBHI.2017.2753464.

Dave, S. *et al.* (2010) 'A secure low-delay protocol for wireless body area networks', 2, pp. 53–72.

Dawson, C. (2002) *Practical research methods: A user-friendly guide to mastering research techniques and projects*. How to books Ltd.

Dawson, C. (2019) *Introduction to Research Methods 5th Edition: A Practical Guide for Anyone Undertaking a Research Project*. Hachette UK.

DEMİR, A. and TATLI, E.İ. (2018) 'Security Analysis of Medical Devices within Wireless Body Area Networks and Mobile Health Applications', *International Journal of Inf.Tech.* [Preprint], (January). Available at: https://doi.org/10.17671/gazibtd.301668.

Dhanvijay, M.M. and Patil, S.C. (2019) 'Internet of Things: A survey of enabling technologies in healthcare and its applications', *Computer Networks,* 153, pp. 113–131. Available at: https://doi.org/10.1016/j.comnet.2019.03.006.

Dharshini, S. and Subashini, M.M. (2017) 'An overview on wireless body area networks', in

Power and Advanced Computing Technologies (i-PACT), pp. 1–10.

Dhaya, R., Kanthavel, R. and Algarni, F. (2020) 'Research perspectives on applications of internet-of-things technology in healthcare WIBSN (wearable and implantable body sensor network)', *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, pp. 279–304.

Dhillon, P.K. and Kalra, S. (2018) 'Multi-factor user authentication scheme for IoT-based healthcare services', *Journal of Reliable Intelligent Environments* [Preprint]. Available at: https://doi.org/10.1007/s40860-018-0062-5.

Dimitriou, T. and Ioannis, K. (2008) 'Security issues in biomedical wireless sensor networks', *2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, pp. 1–5. Available at: https://doi.org/10.1109/ISABEL.2008.4712577.

Dodangeh, P. and Jahangir, A.H. (2018) 'A biometric security scheme for wireless body area networks', *Journal of Information Security and Applications*, 41, pp. 62–74. Available at: https://doi.org/10.1016/j.jisa.2018.06.001.

Easterbrook, S. *et al.* (2008) 'Selecting empirical methods for software engineering research', in *Guide to advanced empirical software engineering*. Springer, pp. 285–311.

Easterby-Smith, M., Thorpe, R. and Jackson, P.R. (2012) *Management research*. Sage.

Eom, D. and Lee, H. (2017) 'A holistic approach to exploring the divided standards landscape in E-Health research', in *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*, pp. 1–7. Available at: https://doi.org/10.23919/ITU-WT.2017.8246985.

EU Commission (2016) *General Data Protection Regulation*. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 13 October 2020).

EU Commission (2017) *Medical Device Regulation*. Available at: https://eur-lex.europa.eu/eli/reg/2017/745/2017-05-05 (Accessed: 13 October 2020).

Fatema, N. and Brad, R. (2014) 'Security Requirements, Counterattacks and Projects in Healthcare Applications Using WSNs - A Review', 2(2), pp. 1–9. Available at: http://arxiv.org/abs/1406.1795.

FDA (2016) *Postmarket Management of Cybersecurity in Medical Devices*. Available at: https://www.fda.gov/media/95862/download (Accessed: 13 October 2020).

FDA (2018) *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Available at: https://www.fda.gov/media/119933/download (Accessed: 13 October 2020).

FDA (2020) *Overview of Device Regulation*. Available at: https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation (Accessed: 9 November 2020).

Feng, Q. *et al.* (2019) 'Lightweight collaborative authentication with key protection for smart electronic health record system', *IEEE Sensors Journal*, 20(4), pp. 2181–2196.

Flick, U. (2014) *An introduction to qualitative research*. sage.

Fotouhi, H. *et al.* (2016) 'Communication and Security in Health Monitoring Systems - A Review', *Proceedings - International Computer Software and Applications Conference*, 1, pp. 545–554. Available at: https://doi.org/10.1109/COMPSAC.2016.8.

Fragopoulos, A.G., Gialelis, J. and Serpanos, D. (2010) 'Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures', *12th IEEE International Conference on e-Health Networking, Application and Services* [Preprint]. Available at:

https://doi.org/10.1109/HEALTH.2010.5556580.

G. Thamilarasu (2015) ‘Genetic algorithm based intrusion detection system for wireless body area networks’, pp. 160–165. Available at: https://doi.org/10.1109/ISCC.2015.7405510.

Garrabrants, W.M. *et al.* (1990) ‘CERTS: a comparative evaluation method for risk management methodologies and tools’, in *[1990] Proceedings of the Sixth Annual Computer Security Applications Conference,* pp. 251–257.

Gebrie, M.T. and Abie, H. (2017) ‘Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth’, in *Proceedings of the 11th European Conference on Software Architecture*.

Gibbert, M. and Ruigrok, W. (2010) ‘The “‘what’”and “‘how’”of case study rigor: Three strategies based on published work’, *Organizational research methods*, 13(4), pp. 710–737.

Gilman, E. and Barth, D. (2017) *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. 1st edn. O’Reilly Media, Inc.

Given, L.M. (2008) *The Sage encyclopedia of qualitative research methods*. Sage publications.

Golafshani, N. (2003) ‘Understanding reliability and validity in qualitative research’, *The qualitative report,* 8(4), pp. 597–607.

Guan, T., Gui, Z. and Ji, S. (2018) ‘Anonymous and certificateless remote data communication protocol for WBANs’, *Proceedings - 2018 1st International Cognitive Cities Conference, IC3 2018,* pp. 154–159. Available at: https://doi.org/10.1109/IC3.2018.00-39.

Guglielmi, A. V *et al.* (2021) ‘Information theoretic key agreement protocol based on ECG signals’, in *2021 IEEE Global Communications Conference (GLOBECOM),* pp. 1–6.

Hadjem, M. *et al.* (2013) ‘Early detection of Myocardial Infarction using WBAN’, *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom 2013*, (Healthcom), pp. 135–139. Available at: https://doi.org/10.1109/HealthCom.2013.6720654.

Hajar, M.S., Al-Kadri, M.O. and Kalutarage, H.K. (2021) ‘A survey on wireless body area networks: Architecture, security challenges and research opportunities’, *Computers \& Security*, 104, p. 102211.

Hameed, S.S. *et al.* (2021) ‘A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches’, *PeerJ Computer Science,* 7, p. e414.

Han, N.D. *et al.* (2014) ‘A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks’, *Information Sciences,* 284, pp. 157–166. Available at: https://doi.org/https://doi.org/10.1016/j.ins.2014.03.126.

Hariharan, U., Rajkumar, K. and Ponmalar, A. (2021) ‘WBAN for e-Healthcare Application: Systematic Review, Challenges, and Counter Measures’, in *2021 International Conference on Computer Communication and Informatics (ICCCI),* pp. 1–7.

Hasan, K. *et al.* (2019) ‘A comprehensive review of wireless body area network’, *Journal of Network and Computer Applications,* 143, pp. 178–198.

Hathaliya, J.J. *et al.* (2019) ‘Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach’, *Computers and Electrical Engineering*, 76, pp. 398–410. Available at: https://doi.org/10.1016/j.compeleceng.2019.04.017.

Hathaliya, J.J. and Tanwar, S. (2020) ‘An exhaustive survey on security and privacy issues in

Healthcare 4.0', *Computer Communications*, 153, pp. 311–335.

Al Hayajneh, A. *et al.* (2020) 'Security of broadcast authentication for cloud-enabled wireless medical sensor devices in 5G networks', *Computer and Information Science,* 13(2), pp. 1–13.

He, D. *et al.* (2014) 'Lightweight and confidential data discovery and dissemination for wireless body area networks', *IEEE Journal of Biomedical and Health Informatics*, 18(2), pp. 440–448. Available at: https://doi.org/10.1109/JBHI.2013.2293620.

He, D. *et al.* (2017) 'Anonymous authentication for wireless body area networks with provable security', *IEEE Systems Journal*, 11(4), pp. 2590–2601. Available at: https://doi.org/10.1109/JSYST.2016.2544805.

Hevner, A.R. *et al.* (2004) 'Design Science in Information Systems Research', *MIS Q.*, 28(1), pp. 75–105. Available at: http://dl.acm.org/citation.cfm?id=2017212.2017217.

HIPAA (2020) *Security Rule*. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (Accessed: 10 October 2020).

Holden, W.L. (2014) 'Bridging the Culture Gap Between Healthcare IT and Medical Device Development', *Biomedical Instrumentation & Technology*, 48(s2), pp. 22–28. Available at: https://doi.org/10.2345/0899-8205-48.s2.22.

Hong, J. *et al.* (2019) 'A combined public-key scheme in the case of attribute-based for wireless body area networks', *Wireless Networks*, 25(2), pp. 845–859. Available at: https://doi.org/10.1007/s11276-017-1597-8.

Hosseini-Khayat, S. (2011) 'A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices', *2011 5th International Symposium on Medical Information and Communication Technology, ISMICT 2011*, pp. 6–9. Available at: https://doi.org/10.1109/ISMICT.2011.5759785.

Huang, C., Lee, H. and Hoon, D. (2012) 'A privacy-strengthened scheme for E-healthcare monitoring system', *Journal of medical systems*, pp. 2959–2971. Available at: https://doi.org/10.1007/s10916-011-9774-2.

Huang, J. and Fan, C. (2016) 'Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments', *Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services.*, pp. 88–93.

Huang, R. (2015) 'Prospect of Wireless Body Area Network Technology', (Esac), pp. 246–249. Available at: https://doi.org/10.2991/esac-15.2015.61.

Hubbard, D.W. (2020) *The failure of risk management: Why it's broken and how to fix it*. John Wiley \& Sons.

Hussain, A. *et al.* (2021) 'Security framework for IoT based real-time health applications', *Electronics*, 10(6), p. 719.

Hussain, M. *et al.* (2019) 'Authentication techniques and methodologies used in wireless body area networks', *Journal of Systems Architecture*, 101, p. 101655.

Hussien, Z.A. *et al.* (2016) 'Secure and efficient e-health scheme based on the Internet of Things', *2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1–6. Available at: https://doi.org/10.1109/ICSPCC.2016.7753621.

Ibrahim, M.H. *et al.* (2016) 'Secure anonymous mutual authentication for star two-tier wireless body area networks', *Computer Methods and Programs in Biomedicine*, 135(July), pp. 37–50. Available at: https://doi.org/10.1016/j.cmpb.2016.07.022.

IEC 62304 (2019) *Health software - Software life cycle processes*.

IEC 80001-1 (2015) *Application of risk management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities and activities*.

IEC 80001-2-2 (2011) *Application of risk management for IT-networks incorporating medical devices-Guidance for the disclosure and communication of medical device security needs, risks and control, International Electrotechnical Committee*.

IEC 80001-5-1 (2020) *IEC 80001-5-1: Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software - Part 5-1: Security - Activities in the product lifecycle*.

IEEE 802.15.6 (2012) *IEEE standard for local and metropolitan area networks. Part 15.6, Wireless body area networks*. Available at: https://ieeexplore-ieee-org.ezproxy.uwtsd.ac.uk/document/6161600.

Iivari, J. and Venable, J.R. (2009) 'Action research and design science research-Seemingly similar but decisively dissimilar'.

Iqbal, J., Amin, N.U. and Umar, A.I. (2013) 'Authenticated key agreement and cluster head selection for Wireless Body Area Networks', *2nd National Conference on Information Assurance (NCIA)*, pp. 113–117. Available at: https://doi.org/10.1109/NCIA.2013.6725334.

Islam, S.M.R. *et al.* (2015) 'The internet of things for health care: a comprehensive survey', *IEEE Access*, 3, pp. 678–708. Available at: https://doi.org/10.1109/ACCESS.2015.2437951.

ISO/IEC 27002 (2017) *Information technology — Security techniques — Code of practice for information security controls*.

ISO/IEC 80001-2-8 (2016) *Application of risk management for IT-networks incorporating medical devices Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2*.

ISO 11770 (2018) *BS ISO/IEC 11770-2:2018 IT Security techniques. Key management. Mechanisms using symmetric techniques*.

ISO 14971 (2018) *Medical devices - Application of risk management to medical devices, International Standard*.

ISO 15446 (2017) *Information technology — Security techniques — Guidance for the production of protection profiles and security targets*.

ISO 27005 (2015) *ISO:27005 Information technology — Security techniques — Information security risk management*.

ISO 27799:2008 (2016) *Health informatics — Information security management in health using ISO / IEC 27002, ISO*.

Iyengar, A., Kundu, A. and Pallis, G. (2018) 'Healthcare informatics and privacy', *IEEE Internet Computing*, 22(2), pp. 29–31. Available at: https://doi.org/10.1109/MIC.2018.022021660.

Izza, S., Benssalah, M. and Ouchikh, R. (2019) 'Security Improvement of the Enhanced 1-round Authentication Protocol for Wireless Body Area Networks', *Proceedings of the 2018 International Conference on Applied Smart Systems, ICASS 2018*, (November), pp. 1–6. Available at: https://doi.org/10.1109/ICASS.2018.8652036.

Jang, C., Lee, D.-G. and Han, J. (2008) 'A proposal of security framework for wireless body area network', in *2008 Int.Conference on Security Technology*, pp. 202–205. Available at:

https://doi.org/10.1109/SecTech.2008.32.

Jang, C.S. *et al.* (2011) ‘Hybrid security protocol for wireless body area networks’, *Wireless Communications and Mobile Computing*, 11(2), pp. 277–288.

Järvinen, P. (2012) ‘On boundaries between field experiment, action research and design research’.

Javadi, S.S. and Razzaque, M.A. (2013) ‘Security and privacy in wireless body area networks for health care applications’, *Wireless Networks and Security*, 26(3), pp. 165–187. Available at: https://doi.org/10.1007/978-3-642-36169-2_6.

Jeedella, J.S.Y. and Al-Qutayri, M. (2017) ‘Technological Solutions for Smart Homes’, in J. van Hoof, G. Demiris, and E.J.M. Wouters (eds) *Handbook of Smart Homes, Health Care and Well-Being*. Cham: Springer International Publishing, pp. 1–13. Available at: https://doi.org/10.1007/978-3-319-01904-8_47-1.

Jiang, Q. *et al.* (2019) ‘Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network’, *IEEE Transactions on Emerging Topics in Computing*, 9(2), pp. 839–853. Available at: https://doi.org/10.1109/TETC.2019.2949137.

Jiang, W., Tan, J. and Liu, W. (2019) ‘An Internal Node Reprogrammable Security Scheme Based on IEEE 802.15.6 in Wireless Body Area Networks’, pp. 285–289. Available at: https://doi.org/10.1145/3291842.3291862.

Jimenez, J.I., Jahankhani, H. and Kendzierskyj, S. (2020) ‘Health care in the cyberspace: Medical cyber-physical system and digital twin challenges’, in *Digital twin technologies and smart cities*. Springer, pp. 79–92.

Kale, S.S. and Bhagwat, D.S. (2018) ‘A Secured IoT Based Webcare Healthcare Controlling System using BSN’, in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, pp. 816–821.

Kamoona, M.A. and Azzazi, A. (2018) ‘Importance of WBAN and Its Security : An Overview’, (8), pp. 30–34.

Kang, J. and Adibi, S. (2015) ‘A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN)’, in R. Doss, S. Piramuthu, and W. ZHOU (eds) *Future Network Systems and Security*. Cham: Springer International Publishing, pp. 61–83.

Kang, J.J. (2020) ‘Systematic analysis of security implementation for internet of health things in mobile health networks’, in *Data Science in Cybersecurity and Cyberthreat Intelligence*. Springer, pp. 87–113.

Kanjee, M.R. and Liu, H. (2016) ‘Authentication and key relay in medical cyber-physical systems’, *Security and Communication Networks*, pp. 874–885. Available at: https://doi.org/10.1002/sec.1009.

Karande, S.N. and Lohiya, G.B. (2015) ‘Trustworthiness of Wireless Body Area Networks (WBANs) and Medical Devices in Healthcare Applications’, 4(3), pp. 497–503.

Karmakar, K. *et al.* (2018) ‘WBAN Security: Study and implementation of a biological key based framework’, *Proceedings of 5th International Conference on Emerging Applications of Information Technology, EAIT 2018*, pp. 1–6. Available at: https://doi.org/10.1109/EAIT.2018.8470409.

Karthikeyan, M. V. and Martin Leo Manickam, J. (2016) ‘Security issues in wireless body area networks: In bio-signal input fuzzy security model: A survey’, *Research Journal of Pharmaceutical, Biological and Chemical Sciences*, 7(6), pp. 1755–1773.

Kasyoka, P., Kimwele, M. and Angolo, S.M. (2020) ‘Towards an efficient certificateless access control scheme for wireless body area networks’, *Wireless Personal Communications*, 115(2), pp. 1257–1275.

Kaur, M. (2015) ‘A Study on Networking Techniques of WBAN System’.

Kavitha, K.C. and Perumalraja, R. (2014) ‘Smart wireless healthcare monitoring for drivers community’, *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*, pp. 1105–1108. Available at: https://doi.org/10.1109/ICCSP.2014.6950019.

Khalil, B. and Naja, N. (2019) ‘A Framework for Security Analytics of WBAN/WLAN Healthcare Network’, *2018 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2018*, pp. 314–319. Available at: https://doi.org/10.1109/ITMC.2018.8691294.

Khan, R.A. (2018) ‘The state-of-the-art wireless body area sensor networks : A survey’, 14(1204). Available at: https://doi.org/10.1177/1550147718768994.

Khanna, P. (2018) ‘Positivism and Realism’, in P. Liamputtong (ed.) *Handbook of Research Methods in Health Social Sciences*. Singapore: Springer Singapore, pp. 1–18. Available at: https://doi.org/10.1007/978-981-10-2779-6_59-1.

Khernane, N., Potop-Butucaru, M. and Chaudet, C. (2017) ‘BANZKP: A Secure Authentication Scheme Using Zero Knowledge Proof for WBANs’, *Proceedings - 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016*, pp. 307–315. Available at: https://doi.org/10.1109/MASS.2016.046.

Kim, D. and Solomon, M.G. (2021) *Fundamentals of information systems security*. Third. Jones \& Bartlett Publishers.

Kitchenham, B. and Charters, S. (2007) ‘Guidelines for performing systematic literature reviews in software engineering’, *Engineering*, 45(4ve), p. 1051. Available at: https://doi.org/10.1145/1134285.1134500.

Ključnikov, A., Mura, L. and Sklenár, D. (2019) ‘Information security management in SMEs: factors of success’, *Entrepreneurship and Sustainability Issues*, 6(4), p. 2081.

Kołodziej, J. *et al.* (2019) ‘Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds’, in J. Kołodziej and H. González-Vélez (eds) *High-Performance Modelling and Simulation for Big Data Applications: Selected Results of the COST Action IC1406 cHiPSet*. Cham: Springer International Publishing, pp. 279–306. Available at: https://doi.org/10.1007/978-3-030-16272-6_10.

Kompara, M. and Hölbl, M. (2018) ‘Survey on security in intra-body area network communication’, *Ad Hoc Networks*, 70, pp. 23–43. Available at: https://doi.org/https://doi.org/10.1016/j.adhoc.2017.11.006.

Kompara, M., Islam, S.H. and Hölbl, M. (2019) ‘A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs’, *Computer Networks*, 148, pp. 196–213. Available at: https://doi.org/10.1016/j.comnet.2018.11.016.

Kotz, D. (2011) ‘A threat taxonomy for mHealth privacy’, in *3rd International Conference on Communication Systems and Networks, COMSNETS*, pp. 1–6. Available at: https://doi.org/10.1109/COMSNETS.2011.5716518.

Kumar, D. *et al.* (2019) ‘General Outlook of Wireless Body Area Sensor Networks’, in *International Conference on Advances in Computing and Data Sciences*, pp. 58–67.

Kumar, M. and Chand, S. (2020) ‘A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network’, *IEEE Systems Journal*, 15(2), pp. 2779–2786. Available at: https://doi.org/10.1109/jsyst.2020.2990749.

Kumar, P. and Lee, H.J. (2012) ‘Security issues in healthcare applications using wireless medical sensor networks: A survey’, *Sensors*, 12(1), pp. 55–91. Available at: https://doi.org/10.3390/s120100055.

Kumar, P., Lee, S.G. and Lee, H.J. (2011) ‘A user authentication for healthcare application using wireless medical sensor networks’, *Proc.- 2011 IEEE International Conference on HPCC 2011 - 2011 IEEE International Workshop on FTDCS 2011 -Workshops of the 2011 Int. Conf. on UIC 2011- Workshops of the 2011 Int. Conf. ATC 2011*, 1, pp. 647–652. Available at: https://doi.org/10.1109/HPCC.2011.92.

Kumar Panigrahy, S. *et al.* (2019) ‘Comparative study of ECG-based key agreement schemes in wireless body sensor networks’, in *Recent findings in intelligent computing techniques*. Springer, pp. 151–161.

Kwak, K.S., Ullah, S. and Ullah, N. (2010) ‘An overview of IEEE 802.15. 6 standard’, in *3rd ISABEL*, pp. 1–6. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5702867.

Kyaw, A.K. and Cusack, B. (2014) ‘Security challenges in pervasive wireless medical systems and devices’, *2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy), HONET-PfE 2014*, pp. 178–185. Available at: https://doi.org/10.1109/HONET.2014.7029386.

Langone, M., Setola, R. and Lopez, J. (2017) ‘Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method’, *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 304–309. Available at: https://doi.org/10.1109/COMPSAC.2017.96.

Latré, B. *et al.* (2011) ‘A survey on wireless body area networks’, *Wireless Networks*, 17(1), pp. 1–18. Available at: https://doi.org/10.1007/s11276-010-0252-4.

LeCompte, M.D. and Schensul, J.J. (1999) *Designing and conducting ethnographic research*. Rowman Altamira.

Lee, Y.S., Alasaarela, E. and Lee, H. (2014) ‘Secure key management scheme based on ECC algorithm for patient’s medical information in healthcare system’, *International Conference on Information Networking*, pp. 453–457. Available at: https://doi.org/10.1109/ICOIN.2014.6799723.

Li, F. and Hong, J. (2016) ‘Efficient certificateless access control for wireless body area networks’, *IEEE Sensors Journal*, 16(13), pp. 5389–5396. Available at: https://doi.org/10.1109/JSEN.2016.2554625.

Li, M. *et al.* (2013) ‘Secure Ad Hoc Trust Initialization and Key Management in Wireless Body Area Networks’, *ACM Trans. Sen. Netw.*, 9(2), pp. 18:1--18:35. Available at: https://doi.org/10.1145/2422966.2422975.

Li, M., Lou, W. and Ren, K. (2010) ‘Data security and privacy in wireless body area networks’, *IEEE Wireless Communications*, 17(1), pp. 51–58. Available at: https://doi.org/10.1109/MWC.2010.5416350.

Li, T., Zheng, Y. and Zhou, T. (2017) ‘Efficient Anonymous Authenticated Key Agreement Scheme for Wireless Body Area Networks’, *Security and Communication Networks*, 2017. Available at: https://doi.org/10.1155/2017/4167549.

Li, W. and Zhu, X. (2015) 'Recommendation-based trust management in body area networks for mobile healthcare', *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, (1), pp. 515–516. Available at: https://doi.org/10.1109/MASS.2014.85.

Li, X. *et al.* (2018) 'Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors', *Telecommunication Systems*, 67(2), pp. 323–348. Available at: https://doi.org/10.1007/s11235-017-0340-1.

Li, Z. and Zhou, Y. (2018) 'Secure and achievable heterogeneous access control scheme for wireless body area networks', *Communications in Computer and Information Science*, 879, pp. 190–198. Available at: https://doi.org/10.1007/978-981-13-3095-7_15.

Lichtenstein, S. (1996) 'Factors in the selection of a risk assessment method', *Information Management \& Computer Security* [Preprint].

Liu, J. (2010) 'Hybrid security mechanisms for wireless body area networks', in *Second Int.Conf. on Ubiquitous and Future Networks (ICUFN)*, pp. 98–103. Available at: https://doi.org/10.1109/ICUFN.2010.5547221.

Liu, J. *et al.* (2014) 'Certificateless remote anonymous authentication schemes for wirelessbody area networks', *IEEE Transactions on Parallel and Distributed Systems*, 25(2), pp. 332–342. Available at: https://doi.org/10.1109/TPDS.2013.145.

Liu, X. *et al.* (2016) 'A secure medical information management system for wireless body area networks', *KSII Transactions on Internet and Information Systems*, 10(1), pp. 221–237. Available at: https://doi.org/10.3837/tiis.2016.01.013.

Liu, X., Jin, C. and Li, F. (2018) 'An Improved Two-Layer Authentication Scheme for Wireless Body Area Networks', *Journal of Medical Systems*, 42(8). Available at: https://doi.org/10.1007/s10916-018-0990-x.

Liu, X., Zhang, R. and Zhao, M. (2019) 'A robust authentication scheme with dynamic password for wireless body area networks', *Computer Networks*, 161, pp. 220–234.

Lofty, A.N. (no date) 'Fundamental Security Challenges in Internet of Things Healthcare Services', pp. 1–6.

MacMahon, S.T., Cooper, T. and McCaffery, F. (2018) 'Revising IEC 80001-1: Risk management of health information technology systems', *Computer Standards & Interfaces*, 60, pp. 67–72.

Mainanwal, V., Gupta, M. and Upadhayay, S.K. (2015) 'A survey on wireless body area network: Security technology and its design methodology issue', *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, (I), pp. 1–5. Available at: https://doi.org/10.1109/ICIIECS.2015.7193088.

Manju, M. and others (2020) 'Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications.', *Indian Journal of Public Health Research \& Development*, 11(6).

Mantas, G., Lymberopoulos, D. and Komninos, N. (2009) 'Integrity mechanism for eHealth tele-monitoring system in smart home environment', *Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009*, pp. 3509–3512. Available at: https://doi.org/10.1109/IEMBS.2009.5334524.

Mapoka, T. *et al.* (2018) 'Secure Mutual Self-Authenticable Mechanism for Wearable

Devices', *International Journal for Information Security Research*, 6(1), pp. 625–635. Available at: https://doi.org/10.20533/ijisr.2042.4639.2016.0072.

March, S.T. and Smith, G.F. (1995) 'Design and natural science research on information technology', *Decision support systems*, 15(4), pp. 251–266.

Mariani, D.M.R. and Mohammed, S. (2015) 'Cybersecurity challenges and compliance issues within the US healthcare sector', *International Journal of Business and Social Research*, 5(02), pp. 55–66.

Marketresearchfuture (2021) 'Body Area Network Market'. Available at: https://www.globenewswire.com/news-release/2021/08/12/2279692/0/en/Body-Area-Network-Market-to-Touch-USD-21-Billion-at-13-CAGR-by-2025-Report-by-Market-Research-Future-MRFR.html (Accessed: 20 August 2021).

Masdari, M., Ahmadzadeh, S. and Bidaki, M. (2017) 'Key management in wireless Body Area Network: Challenges and issues', *Journal of Network and Computer Applications*, 91, pp. 36–51. Available at: https://doi.org/https://doi.org/10.1016/j.jnca.2017.04.008.

Masood, I. *et al.* (2018) 'Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure', *Wireless Communications and Mobile Computing*, 2018, pp. 1–23. Available at: https://doi.org/10.1155/2018/2143897.

Mehmood, G. *et al.* (2020) 'A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks', *IEEE Access*, 8, pp. 131397–131413. Available at: https://doi.org/10.1109/ACCESS.2020.3007405.

Mekki, N. *et al.* (2018) 'A Privacy-Preserving Scheme Using Chaos Theory for Wireless Body Area Network', *2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018*, pp. 774–779. Available at: https://doi.org/10.1109/IWCMC.2018.8450293.

Miao, F. *et al.* (2009) 'A novel biometrics based security solution for body sensor networks', *Proceedings of the 2009 2nd International Conference on Biomedical Engineering and Informatics, BMEI 2009* [Preprint]. Available at: https://doi.org/10.1109/BMEI.2009.5304950.

Minocha, S. (2013) 'WBAN and its Applications', *International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)*, 02(01), pp. 11–14.

Mohd, B.J., Hayajneh, T. and Vasilakos, A. V (2015) 'A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues', *Journal of Network and Computer Applications*, 58, pp. 73–93. Available at: https://doi.org/https://doi.org/10.1016/j.jnca.2015.09.001.

Movassaghi, Samaneh *et al.* (2014) 'Wireless body area networks: A survey', *IEEE Communications Surveys and Tutorials*, 16(3), pp. 1658–1686. Available at: https://doi.org/10.1109/SURV.2013.121313.00064.

Movassaghi, S *et al.* (2014) 'Wireless Body Area Networks: A Survey', *Ieee Communications Surveys and Tutorials*, 16(3), pp. 1658–1686. Available at: https://doi.org/10.1109/surv.2013.121313.00064.

Mucchi, L. *et al.* (2019) 'An Overview of Security Threats, Solutions and Challenges in WBANs for Healthcare', *International Symposium on Medical Information and Communication Technology, ISMICT*, 2019-May, pp. 4–9. Available at: https://doi.org/10.1109/ISMICT.2019.8743798.

Muhammad, K. ur R.R.S. *et al.* (2009) 'BARI: A Distributed Key Management Approach for Wireless Body Area Networks', *Sensors*, 10(4), pp. 3911–3933. Available at: https://doi.org/10.3390/s100403911.

Muka, R., Yildrim-Yayilgan, S. and Sevrani, K. (2019) 'Security Analysis of Wireless BAN in e-Health', *International Journal of Business & Technology*, 5(2), pp. 1–7. Available at: https://doi.org/10.33107/ijbte.2017.5.2.02.

MurtazaRashidAlMasud, S. (2013) 'Study and Analysis of Scientific Scopes, Issues and Challenges towards Developing a Righteous Wireless Body Area Network', *International Journal of Computer Applications*, 74(6), pp. 46–56. Available at: https://doi.org/10.5120/12893-0061.

Mwitende, G. *et al.* (2020) 'Authenticated key agreement for blockchain-based WBAN', *Telecommunication Systems*, 74(3), pp. 347–365.

N., S. and H., R. (2016) 'Recent Research on Wireless Body Area Networks: A Survey', *International Journal of Computer Applications*, 142(11), pp. 42–48. Available at: https://doi.org/10.5120/ijca2016909893.

Naik, M.R.K. and Samundiswary, P. (2016) 'Wireless body area network security issues — Survey', *Int. Conf. on Control, Instr., Communication and Computational Technologies (ICCICCT)*, pp. 190–194. Available at: https://doi.org/10.1109/ICCICCT.2016.7987943.

Narwal, B. and Mohapatra, A.K. (2020) 'SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks', *Wireless Personal Communications*, 113(4), pp. 1985–2008.

Negra, R., Jemili, I. and Belghith, A. (2016) 'Wireless Body Area Networks: Applications and Technologies', *Procedia Computer Science*, 83, pp. 1274–1281. Available at: https://doi.org/10.1016/j.procs.2016.04.266.

Networks (2018) 'ECG-Based Secure Healthcare Monitoring System in Body Area Networks', *2018 Fourth International Conference on Biosignals, Images and Instrumentation (ICBSII)*, 16(2), pp. 171–193. Available at: https://www.cst.com/Content/Events/downloads/euc2013/3-1-4_CST_EUC.pdf.

Nidhya, R. and Karthik, S. (2019) 'Security and privacy issues in remote healthcare systems using wireless body area networks', in *Body Area Network Challenges and Solutions*. Springer, pp. 37–53.

Niksaz, P. (2015) 'Wireless Body Area Networks: Attacks and Countermeasures', *International Journal of Scientific & Engineering Research*, 6(9), pp. 556–568. Available at: http://www.ijser.org.

NIST:800-30 (2012) *Guide for Conducting Risk Assessments, NIST*. Available at: https://doi.org/10.6028/NIST.SP.800-30r1.

NIST (2013) 'NIST 800-53 Revision 4'. Available at: https://doi.org/10.6028/NIST.SP.800-53Ar4.

NIST (2020) *NVD - CVSS v3 Calculator*. Available at: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (Accessed: 19 August 2020).

NIST CSF (2021) *NIST Cybersecurity Framework.* Available at: https://www.nist.gov/cyberframework (Accessed: 6 July 2021).

NIST RMF (2023) *NIST Risk Management Framework.*

NIST SP 800-61 (2024) *NIST SP 800-61 Rev. 3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*.

NIST SP800-53 (2020) *Security and privacy controls for federal information systems and organizations, NIST Special Publication*.

NISTIR 8062 (2017) *NISTIR 8062: An introduction to privacy engineering and risk management in federal systems, NIST Interagency Report*. Available at: https://doi.org/10.6028/NIST.IR.8062.

Oates, B.J. (2006) *Researching information systems and computing*. SAGE.

Obaidat, M.A. *et al.* (2020) 'A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures', *Computers*, 9(2), p. 44.

Odesile, A. and Thamilarasu, G. (2017) 'Distributed intrusion detection using mobile agents in wireless body area networks', *Proceedings - 2017 7th International Conference on Emerging Security Technologies, EST 2017,* pp. 144–149. Available at: https://doi.org/10.1109/EST.2017.8090414.

Oladimeji, E.A., Supakkul, S. and Chung, L. (2006) 'Security threat modeling and analysis: A goal-oriented approach', in *Proc. of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006),* pp. 13–15.

Olakanmi, O.O. (2017) 'Lightweight Security and Privacy Scheme for Wireless Body Area Network in E-Health System', *International Journal of Information Security Science,* 6(3), pp. 26–38. Available at: https://www.semanticscholar.org/paper/Lightweight-Security-and-Privacy-Scheme-for-Body-in-Olakanmi/b34866031740e5249fb54d673ce3869eac5600b6.

Omoogun, M. *et al.* (2017) 'When eHealth meets the internet of things: Pervasive security and privacy challenges', *2017 International Conference on Cyber Security And Protection Of Digital Services, Cyber Security 2017* [Preprint]. Available at: https://doi.org/10.1109/CyberSecPODS.2017.8074857.

OWASP Authentication (no date) *Authentication · OWASP Cheat Sheet Series*. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (Accessed: 22 October 2019).

Paquette, A., Painter, F. and Jackson, J.L. (2011) 'Management and risk assessment of wireless medical devices in the hospital', *Biomedical instrumentation \& technology,* 45(3), pp. 243–248.

Paramita, S. (2020) 'IoT-Based WBAN Health Monitoring System with Security', in *Internet of Things*. CRC Press, pp. 107–120.

Partala, J. *et al.* (2013) 'Security threats against the transmission chain of a medical health monitoring system', *15th Int. Conf. on e-Health Net., Appl. and Serv.,* (Healthcom), pp. 243–248. Available at: https://doi.org/10.1109/HealthCom.2013.6720675.

Pathania, S. and Bilandi, N. (2014) 'Security Issues in Wireless Body Area Network', *International Journal of Computer Science and Mobile Computing,* 3(4), pp. 1171–1178.

Patton, M.Q. (2001) 'Qualitative Research & Evaluation Methods'.

Paul, P.C. *et al.* (2019) 'Analysis of Attacks and Security Requirements for Wireless Body Area Networks-A Systematic Literature Review', in *European Conference on Software Process Improvement,* pp. 439–452.

Paul, P.C. *et al.* (2021) ‘A Data Security And Privacy Risk Management Framework For WBAN Based Healthcare Applications*’, in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops),* pp. 704–710. Available at: https://doi.org/10.1109/PerComWorkshops51409.2021.9431069.

Peffers, K. *et al.* (2007) ‘A design science research methodology for information systems research’, *Journal of management information systems,* 24(3), pp. 45–77.

Picazo-Sanchez, P. *et al.* (2014) ‘Secure publish-subscribe protocols for heterogeneous medical wireless body area networks’, *Sensors (Switzerland),* 14(12), pp. 22619–22642. Available at: https://doi.org/10.3390/s141222619.

Prakash, S. and Mamta (2016) ‘An overview of healthcare perspective based security issues in wireless sensor networks’, in *Comput. for Sust.Global Dev.*, pp. 870–875.

Pramanik, P.K.D., Pareek, G. and Nayyar, A. (2019) *Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards*, *Telemedicine Technologies*. Elsevier Inc. Available at: https://doi.org/10.1016/b978-0-12-816948-3.00014-3.

Prema, L. and Devi, L. (2017) ‘An Efficient Authentication & Light Weight Security in WBAN’, *International Journal of Engineering Science and Computing,* 7(11), pp. 15679–15683. Available at: http://ijesc.org/.

Punj, R. and Kumar, R. (2019) *Technological aspects of WBANs for health monitoring: a comprehensive review*, *Wireless Networks*. Springer US. Available at: https://doi.org/10.1007/s11276-018-1694-3.

Qadri, S.F. *et al.* (2013) ‘Applications, challenges, security of wireless body area networks (WBANs) and functionality of IEEE 802.15. 4/ZIGBEE’, *Science International Lahore,* 25(4), pp. 697–702.

Ragesh, G.K. and Baskaran, K. (2012) ‘CRYPE: Towards Cryptographically Enforced and Privacy Enhanced WBANs’, in *Proceedings of the First International Conference on Security of Internet of Things*. New York, NY, USA: ACM (SecurIT ’12), pp. 204–209. Available at: https://doi.org/10.1145/2490428.2490457.

Ragesh, G.K. and Baskaran, K. (2013) ‘Addressing the Need for Context Awareness and Security Requirements in Wireless Body Area Networks’, *International Journal of Future Computer and Communication,* 1(3), pp. 302–305. Available at: https://doi.org/10.7763/ijfcc.2012.v1.81.

Raju, M.H. *et al.* (2020) ‘Security analysis and a potential layer to layer security solution of medical cyber-physical systems’, in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Springer, pp. 61–86.

Ramli, S.N. *et al.* (2013) ‘A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)’, *Advanced Communication Technology (ICACT), 2013 15th International Conference*, pp. 998–1001.

Ramli, S.N. and Ahmad, R. (2011) ‘Surveying the wireless body area network in the realm of wireless communication’, in *7th Int. Conference on Information Assurance and Security (IAS),* pp. 58–61.

Ramu, G. (2018) ‘A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter’, *Education and Information Technologies* [Preprint].

Ray, P.P., Dash, D. and Kumar, N. (2020) ‘Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions', *Computer Communications,* 160, pp. 111–131.

Raza, A. *et al.* (2020) 'Comprehensive survey of routing protocols for wireless body area networks (WBANs)', *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital,* pp. 145–178.

Ren, Y. *et al.* (2019) 'Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network', *Sensors,* 19(10), p. 2395. Available at: https://doi.org/10.3390/s19102395.

Researchandmarkets (2021) *Medical Sensor Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026).* Available at: https://www.researchandmarkets.com/reports/4535852/medical-sensor-market-growth-trends-covid-19 (Accessed: 20 May 2021).

Rismanian, F., Hosseinzadeh, M. and Jabbehdari, S. (2017) 'A Review of State-of-the-Art on Wireless Body Area Networks', *International Journal of Advanced Computer Science and Applications*, 8(11), pp. 443–455. Available at: https://doi.org/10.14569/ijacsa.2017.081154.

Robson, C. and McCartan, K. (2016) *Real world research*. John Wiley \& Sons.

Roy, M., Chowdhury, C. and Aslam, N. (2020) 'Security and privacy issues in wireless sensor and body area networks', in *Handbook of computer networks and cyber security*. Springer, pp. 173–200.

Rubin, H. and Rubin, I. (2012) 'Qualitative Interviewing (2nd ed.): The Art of Hearing Data'. Thousand Oaks, California. Available at: https://doi.org/10.4135/9781452226651.

Saarika, U., Sharma, P.K. and Sharma, D. (2016) 'A roadmap to the realization of wireless body area networks: a review', in *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* pp. 439–443.

Saha, M.S. and Anvekar, D.K. (2014) 'State of The Art in WBAN Security & Open Research Issues', (July).

Sahoo, S.S. and Mohanty, S. (2019) 'Chaotic Map based Privacy Preservation User Authentication Scheme for WBANs', *IEEE Region 10 Annual International Conference, Proceedings/TENCON,* 2019-Octob, pp. 1037–1042. Available at: https://doi.org/10.1109/TENCON.2019.8929338.

Saif, S. and Biswas, S. (2019) *Secure Data Transmission Beyond Tier 1 of Medical Body Sensor Network*. Springer Singapore. Available at: https://doi.org/10.1007/978-981-13-1544-2.

Saif, S., Gupta, R. and Biswas, S. (2018) 'Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring', in S. Bhattacharyya et al. (eds) *Advanced Computational and Communication Paradigms*. Singapore: Springer Singapore, pp. 665–674.

Sajid, A. and Abbas, H. (2016) 'Data privacy in cloud-assisted healthcare systems: state of the art and future challenges', *Journal of Medical Systems* [Preprint]. Available at: https://doi.org/10.1007/s10916-016-0509-2.

Salayma, M., Al-dubai, A. and Romdhani, I. (2017) 'Wireless body area network (WBAN): a survey on reliability, fault tolerance, and technologies coexistence', *ACM Computing Surveys,* 50(1), pp. 1–38.

Saleem (2009) 'On the Security Issues in Wireless Body Area Networks', *International Journal of Digital Content Technology and its Applications,* 3(3). Available at:

https://doi.org/10.4156/jdcta.vol3.issue3.22.

Saleem, K. *et al.* (2016) ‘Survey on cybersecurity issues in wireless mesh networks based eHealthcare’, *IEEE 18th International Conference on e-Health Networking, Applications and Services* [Preprint]. Available at: https://doi.org/10.1109/HealthCom.2016.7749423.

Saleem, K., Tan, Z. and Buchanan, W. (2017) ‘Security for Cyber-Physical Systems in Healthcare’, in C. Thuemmler and C. Bai (eds) *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. Cham: Springer International Publishing, pp. 233–251. Available at: https://doi.org/10.1007/978-3-319-47617-9_12.

Saleem, S., Ullah, S. and Kwak, K.S. (2010) ‘Towards security issues and solutions in wireless body area networks’, *6th International Conference on Networked Computing (INC),* pp. 1–4. Available at: https://doi.org/10.1109/ICUFN.2010.5547221.

Saleem, S., Ullah, S. and Kwak, K.S. (2011) ‘A study of IEEE 802.15.4 security framework for wireless body area networks’, *Sensors*, 11(2), pp. 1383–1395. Available at: https://doi.org/10.3390/s110201383.

Salehi, S.A. *et al.* (2016) ‘IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view’, *Proceedings - Asia-Pacific Conference on Communications, APCC 2016*, pp. 523–528. Available at: https://doi.org/10.1109/APCC.2016.7581523.

Salman, S. *et al.* (2013) ‘A non-invasive lung monitoring sensor with integrated body-area network’, *2013 IEEE MTT-S International Microwave Workshop Series on RF and Wireless Technologies for Biomedical and Healthcare Applications, IMWS-BIO 2013 - Proceedings*, (1), pp. 1–3. Available at: https://doi.org/10.1109/IMWS-BIO.2013.6756243.

Sampangi, R. V (2014) ‘HiveSign : Dynamic Message Signatures for Resource-Constrained Wireless Networks’, *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, pp. 33–40.

Sangari, S. and Manickam, M. (2014) ‘Security and Privacy in Wireless Body Area Network’, *Indian Streams Research Journal*, 5(8), pp. 1–7. Available at: https://doi.org/10.9780/22307850.

Santra, T. (2010) ‘Mobile Health Care System for Patient Monitoring’, *Communications in Computer and Information Science*, 101, pp. 695–700. Available at: https://doi.org/10.1007/978-3-642-15766-0_123.

Sarvabhatla, M., Reddy, M.C.M. and Vorugunti, C.S. (2015) ‘A Robust Biometric-Based Authentication Scheme for Wireless Body Area Network Using Elliptic Curve Cryptosystem’, in *Proceedings of the Third International Symposium on Women in Computing and Informatics*. New York, NY, USA: ACM (WCI ’15), pp. 582–587. Available at: https://doi.org/10.1145/2791405.2791465.

Saunders, M., Lewis, P. and Thornhill, A. (2009) *Research methods for business students*. Pearson education.

Sawand, A. *et al.* (2015) ‘Toward energy-efficient and trustworthy eHealth monitoring system’, *China Communications*, 12(1), pp. 46–65. Available at: https://doi.org/10.1109/CC.2015.7084383.

Sawaneh, I.A., Sankoh, I. and Koroma, D.K. (2017) ‘A survey on security issues and wearable sensors in wireless body area network for healthcare system’, in *Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 304–308.

Sein, Maung K. *et al.* (2011) ‘Action design research’, *MIS Quarterly: Management*

Information Systems, 35(1), pp. 37–56. Available at: https://doi.org/10.2307/23043488.

Sein, Maung K *et al.* (2011) 'Action design research', *MIS quarterly*, pp. 37–56.

Seneviratne, S. *et al.* (2017) 'A survey of wearable devices and challenges', *IEEE Communications Surveys and Tutorials*, 19(4), pp. 2573–2620. Available at: https://doi.org/10.1109/COMST.2017.2731979.

Shah, S.M. and Khan, R.A. (2020) 'Secondary use of electronic health record: Opportunities and challenges', *IEEE Access*, 8, pp. 136947--136965.

Shah, S.T.U. *et al.* (2018) 'Internet of Things-Based Healthcare: Recent Advances and Challenges', pp. 153–162. Available at: https://doi.org/10.1007/978-3-319-96139-2_15.

Shankar, S.K., Tomar, A.S. and Tak, G.K. (2015) 'Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSNs', *Procedia Computer Science*, 70, pp. 455–461. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2015.10.078.

Sharma, G. and Kalra, S. (2018) 'A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services', *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 5. Available at: https://doi.org/10.1007/s40998-018-0146-5.

Sharmila, A.H. and Jaisankar, N. (2020) 'E-MHMS: enhanced MAC-based secure delay-aware healthcare monitoring system in WBAN', *Cluster Computing*, 23(3), pp. 1725–1740.

Shen, Jian, Gui, Z., *et al.* (2018a) 'Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks', *Journal of Network and Computer Applications*, 106(September 2017), pp. 117–123. Available at: https://doi.org/10.1016/j.jnca.2018.01.003.

Shen, Jian, Gui, Z., *et al.* (2018b) 'Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks', *Journal of Network and Computer Applications*, 106, pp. 117–123. Available at: https://doi.org/https://doi.org/10.1016/j.jnca.2018.01.003.

Shen, Jian, Chang, S., *et al.* (2018) 'Implicit authentication protocol and self-healing key management for WBANs', *Multimedia Tools and Applications*, pp. 1–21. Available at: https://doi.org/10.1007/s11042-017-5559-z.

Sherali Zeadally, Jesús Téllez Isaac, Z.B. (2016) 'Security attacks and solutions in electronic health (e-health) systems', *Journal of Medical Systems* [Preprint]. Available at: https://doi.org/10.1007/s10916-016-0597-z.

Shuai, M. *et al.* (2020) 'Efficient and privacy-preserving authentication scheme for wireless body area networks', *Journal of Information Security and Applications*, 52, p. 102499.

Sindhu, K. V (2017) 'Trustworthy access control for wireless body area networks', in *Information Communication and Embedded Systems (ICICES)*, pp. 1–5.

Singel, D. (2008) 'A secure cross-layer protocol for multi-hop wireless body area networks', in *International Conference on Ad-Hoc Networks and Wireless*, pp. 94–107.

Singh, R. *et al.* (2020) 'Wireless body area network: An application of IoT and its issuses—A survey', in *Computational Intelligence in Pattern Recognition*. Springer, pp. 285–293.

Siva Bharathi, K.R. and Venkateswari, R. (2019) 'Security Challenges and Solutions for Wireless Body Area Networks', in *Comp., Comm.. and Signal Proc.*, pp. 275–283.

Skierka, I.M. (2018) 'The governance of safety and security risks in connected healthcare', *IET Conference Publications*, pp. 1–12.

Soh, P.J. *et al.* (2015) 'Wearable wireless health monitoring: Current developments, challenges, and future trends', *IEEE Microwave Magazine,* 16(4), pp. 55–70. Available at: https://doi.org/10.1109/MMM.2015.2394021.

Song, Y. and Tan, H. (2020) 'Practical pairing-Free sensor cooperation scheme for cloud-Assisted wireless body area networks', *Cybersecurity,* 3(1), pp. 1–9.

Sowjanya, K., Dasgupta, M. and Ray, S. (2020) 'An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems', *International Journal of Information Security,* 19(1), pp. 129–146.

Spratt, C., Walker, R. and Robinson, B. (2004) *Mixed research methods*. Available at: http://oasis.col.org/bitstream/handle/11599/88/A5 workbook.pdf?sequence=1&isAllowed=y (Accessed: 9 May 2021).

Sridharan, S. and Kiran, G.R. (2013) 'Secure authentication model for online health monitoring system', *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT),* pp. 1–5. Available at: https://doi.org/10.1109/ICCCNT.2013.6726758.

Sridharan, S. and Shrivastava, H. (2014) 'Excogitation of Secure Data Authentication Model for Wireless Body Area Network', pp. 3–5.

Stevovic, J. *et al.* (2013) 'Compliance aware cross-organization medical record sharing', *IFIP/IEEE International Symposium on Integrated Network Management, IM 2013,* pp. 772–775.

Sudha, R. (2021) 'An Emerging Trust-Based Security on Wireless Body Area Network', in *Sustainable Communication Networks and Application*. Springer, pp. 215–226.

Sultana, S. *et al.* (2020) 'A Critical Study on Internet of Medical Things for Secure WBAN', in *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*. IGI Global, pp. 179–197.

Sun, W. *et al.* (2018) 'Security and Privacy in the Medical Internet of Things: A Review', *Security and Communication Networks,* 2018, pp. 1–9. Available at: https://doi.org/10.1155/2018/5978636.

Sundararajan, A., Sarwat, A.I. and Pons, A. (2019) 'A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems', *ACM Computing Surveys,* 52(2), pp. 1–36. Available at: https://doi.org/10.1145/3309550.

Supriya, S. and Padaki, S. (2016) 'Data Security and Privacy Challenges in Adopting Solutions for IOT', *2016 IEEE International Conference on Internet of Things (iThings),* pp. 410–415.

T.MeenaAbarna, K. and Venkatachalapathy, K. (2012) 'Light-weight Security Architecture for IEEE 802. 15. 4 Body Area Networks', *International Journal of Computer Applications,* 47(22), pp. 1–8. Available at: https://doi.org/10.5120/7485-9972.

T, S.V. and K, S.R. (2018) 'A survey overview : on wireless body area network and its various applications', 7, pp. 936–940.

Taha, M.S. *et al.* (2018) 'Wireless Body Area Network revisited', *International Journal of Engineering & Technology,* 7(4), pp. 35–46. Available at: https://doi.org/10.15446/rsap.v18n6.51794.

Tariq, M. (2017) 'Threats, Challenges, Security of Wire Less Body Area Networks (Wban) Using Ieee 802.15.4/Zigbee', *International Journal of Scientific & Engineering Research,* 8(5).

Available at: http://www.ijser.org.

Tayal, A. and Prachi (2013) 'Securing E-healthcare applications with PPS and PDS', *International Conference on Advanced Computing and Communication Technologies, ACCT*, pp. 45–49. Available at: https://doi.org/10.1109/ACCT.2013.20.

Thamilarasu, G. and Odesile, A. (2016) 'Securing wireless body area networks: Challenges, review and recommendations', *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),* pp. 1–7. Available at: https://doi.org/10.1109/ICCIC.2016.7919700.

Thampi, V.V.A. and Gopal, R.K. (2015) 'A review on different encryption algorithms for a wellness tracking system', *Global Conference on Communication Technologies, GCCT 2015,* (Gcct), pp. 817–822. Available at: https://doi.org/10.1109/GCCT.2015.7342776.

Thapa, C. and Camtepe, S. (2021) 'Precision health data: Requirements, challenges and existing techniques for data security and privacy', *Computers in Biology and Medicine,* 129, p. 104130.

Tote, S.S., Khupse, S.M. and Bhutwani, K.S. (2015) 'Data Authentication in Wireless Body Area Network (WBAN) Using A Biometric-Based Security', *International Journal for Research in Emerging Science and Technology,* 2(1), pp. 136–142.

Touhill, G.J. and Touhill, C.J. (2014) *Cybersecurity for executives: A practical guide*. John Wiley \& Sons.

Townsend, K. (2017) *Organizations Challenged with Cybersecurity Framework Implementation*. Available at: https://www.securityweek.com/organizations-challenged-cybersecurity-framework-implementation (Accessed: 10 October 2020).

Trochim, P.W.M.K. (2020) *Research Methods Knowledge Base, Tools and support for product and pricing research - Conjoint.ly*. Conjoint.ly. Available at: https://conjointly.com/kb/ (Accessed: 22 February 2021).

Ullah, I. *et al.* (2021) 'Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN)', *Microprocessors and Microsystems,* 81, p. 103477.

Ullah, S. *et al.* (2012) 'A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions', *Journal of Medical Systems,* 36(3), pp. 1065–1094.

Ullah, S. and Alamri, A. (2013) 'A secure RFID-based WBAN for healthcare applications', *Journal of medical systems* [Preprint]. Available at: https://doi.org/10.1007/s10916-013-9961-4.

Umar, M., Liao, X. and Chen, J. (2019) 'Enhanced BAN-GZKP: Optimal zero knowledge proof based scheme in body area networks', *Proceedings - 2019 International Conference on Networking and Network Applications, NaNA 2019,* pp. 96–101. Available at: https://doi.org/10.1109/NaNA.2019.00026.

Umar, M., Wu, Z. and Liao, X. (2020) 'Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics', *IEEE Access,* 8, pp. 66411–66422. Available at: https://doi.org/10.1109/ACCESS.2020.2985261.

Usman, M. *et al.* (2018) 'Security in wireless body area networks: From in-body to off-body communications', *IEEE Access,* 6, pp. 58064–58074. Available at: https://doi.org/10.1109/ACCESS.2018.2873825.

Vaniprabha, A. and Poongodi, P. (2019) 'Augmented lightweight security scheme with access control model for wireless medical sensor networks', *Cluster Computing*, 22(5), pp. 12495–12505.

Venkatasubramanian, S. and Jothi, V. (2012) 'Integrated authentication and security check with CDMA modulation technique in physical layer of Wireless Body Area Network', *2012 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2012* [Preprint]. Available at: https://doi.org/10.1109/ICCIC.2012.6510239.

Vyas, A. and Pal, S. (2020) 'Preventing security and privacy attacks in WBANs', in *Handbook of computer networks and cyber security*. Springer, pp. 201–225.

Wang, G., Lu, R. and Guan, Y.L. (2019) 'Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System', *IEEE Access*, 7, pp. 33565–33576. Available at: https://doi.org/10.1109/ACCESS.2019.2891775.

Wang, J. *et al.* (2013) 'A research on security and privacy issues for patient related data in medical organization system', *International Journal of Security and its Applications*, 7(4), pp. 287–298.

Wang, J. *et al.* (2018) 'An ASIC Implementation of Security Scheme for Body Area Networks', *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5. Available at: https://doi.org/10.1109/ISCAS.2018.8351098.

Wang, J.C. *et al.* (2016) 'Wireless body area network and its applications', *ISOCC 2015 - International SoC Design Conference: SoC for Internet of Everything (IoE)*, pp. 169–170. Available at: https://doi.org/10.1109/ISOCC.2015.7401772.

Wang, X. and Jin, Z. (2019) 'An Overview of Mobile Cloud Computing for Pervasive Healthcare', *IEEE Access*, 7, pp. 66774–66791. Available at: https://doi.org/10.1109/ACCESS.2019.2917701.

Wazid, M. *et al.* (2017) 'A novel authentication and key agreement scheme for implantable medical devices deployment', *IEEE Journal of Biomedical and Health Informatics*, 22(4), pp. 1299–1309. Available at: https://doi.org/10.1109/JBHI.2017.2721545.

Whitman, M.E., Mattord, H.J. and others (2017) *Principles of information security*. Thomson Course Technology Boston, MA.

Wright, H.K., Kim, M. and Perry, D.E. (2010) 'Validity concerns in software engineering research', in *Proceedings of the FSE/SDP workshop on Future of software engineering research*, pp. 411–414.

Wu, L. *et al.* (2016) 'Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks'. Available at: https://doi.org/10.1007/s10916-016-0491-8.

Wu, T. *et al.* (2017) 'An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications', *IEEE Access*, 5, pp. 11413–11422. Available at: https://doi.org/10.1109/ACCESS.2017.2716344.

Wu, X. (2014) 'A lightweight trust-based access control model in cloud-assisted wireless body area networks', *International Journal of Security and Its Applications*, 8(5), pp. 131–138.

Xu, J. *et al.* (2018) 'Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/https://doi.org/10.1016/j.future.2018.04.018.

Xu, J. *et al.* (2019) 'A hybrid mutual authentication scheme based on blockchain technology for WBANs', in *International Conference on Blockchain and Trustworthy Systems*, pp. 350–

362.

Xu, Z. *et al.* (2019) ‘A lightweight mutual authentication and key agreement scheme for medical internet of things’, *IEEE Access*, 7, pp. 53922–53931. Available at: https://doi.org/10.1109/ACCESS.2019.2912870.

Yang, X. *et al.* (2021) ‘Efficient and Anonymous Authentication for Healthcare Service with Cloud based WBANs’, *IEEE Transactions on Services Computing*, 00(00). Available at: https://doi.org/10.1109/TSC.2021.3059856.

Yaqoob, T., Abbas, H. and Atiquzzaman, M. (2019) ‘Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices − A Review’, *IEEE Communications Surveys and Tutorials* [Preprint]. Available at: https://doi.org/10.1109/COMST.2019.2914094.

Yaseen, M. *et al.* (2018) ‘Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art’, *Telematics and Informatics*, 35(4), pp. 702–726. Available at: https://doi.org/10.1016/j.tele.2017.08.005.

Yin, L. *et al.* (2017) ‘Security-aware attribute-based access control for fog-based eldercare system’, in *Com. and Commun. (ICCC)*, pp. 2680–2684.

Zhang, X. *et al.* (2019) ‘CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors’, *IEEE Transactions on Cloud Computing* [Preprint].

Zhou, J., Cao, Z., Dong, X., Xiong, N. and Vasilakos, A. V. (2015) ‘4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks’, *Information Sciences*, 314, pp. 255–276. Available at: https://doi.org/10.1016/j.ins.2014.09.003.

Zhou, J., Cao, Z., Dong, X., Xiong, N. and Vasilakos, A. V (2015) ‘4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks’, *Information Sciences*, 314, pp. 255–276. Available at: https://doi.org/https://doi.org/10.1016/j.ins.2014.09.003.

Zhou, J., Cao, Z. and Dong, X. (2013) ‘BDK : Secure and Efficient Biometric based Deterministic Key Agreement in Wireless Body Area Networks’, *Proceedings of the 8th international conference on body area networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)*, 1.

Zhu, Y. *et al.* (2009) ‘A lightweight policy system for body sensor networks’, *IEEE Transactions on Network and Service Management*, 6(3), pp. 137–148. Available at: https://doi.org/10.1109/TNSM.2009.03.090301.

Zhu, Y. *et al.* (2012) ‘Vesta: A secure and autonomic system for pervasive healthcare’. Available at: https://doi.org/10.4108/icst.pervasivehealth2009.5939.

Zou, S. *et al.* (2017) ‘A Survey on Secure Wireless Body Area Networks’, *Security and Communication Networks*, 2017. Available at: https://doi.org/10.1155/2017/3721234.

Appendix A Mapping of Occurrence of Security and Privacy Requirements for WBAN Applications

Mapping of occurrence of security and privacy requirements for WBAN applications in current literature:

Ref no	Data Confidentiality	Data Integrity	Authentication	Non-repudiation	Access Control	Availability	Privacy	Encryption/ Cryptography	Key Management	Data Freshness	Firewall	Accountability	Revocability	Intrusion Detection	Trust Management	Forward secrecy / Backward secrecy	Resilience	Physical Protection	Auditability	Client Platform Security	Anonymity	Regulations and compliance requirement
P1	x	x	x	x	x	x						x	x									
P2	x	x	x			x	x		x	x				x	x		x					
P3	x	x				x																
P4		x	x		x			x			x											
P5	x	x	x			x								x	x							
P6	x	x	x	x	x	x	x	x	x	x				x								
P7	x	x				x																
P8	x	x			x					x												
P9	x	x							x	x												
P10	x		x				x	x														
P11	x	x	x			x			x	x		x		x	x							x
P12	x	x	x	x	x	x	x					x	x									
P13	x	x	x			x	x	x	x	x												
P14	x	x	x	x	x	x	x	x	x	x		x										
P15	x	x	x	x		x	x			x			x			x					x	
P16	x	x	x	x	x		x	x				x							x	x	x	
P17	x	x	x			x																
P18	x	x	x	x			x		x							x						
P19	x	x	x				x	x														
P20	x	x	x	x	x	x	x	x	x	x												
P21	x	x	x						x							x						
P22			x		x				x									x				
P23	x	x	x			x										x					x	
P24	x	x	x	x	x	x	x															
P25			x																			
P26	x	x	x			x			x	x												
P27	x	x	x		x																	
P28	x	x	x	x	x																	
P29			x		x			x	x													
P30	x	x	x	x	x	x				x							x					
P31	x	x	x	x	x	x						x	x									
P32	x	x				x																
P33	x	x	x	x																		
P34			x			x	x															
P35	x	x				x	x															
P36		x	x					x		x												
P37	x	x	x		x	x		x	x	x					x		x					
P38	x	x	x																			
P39	x	x	x							x												
P40	x	x	x				x															
P41	x	x	x						x								x				x	
P42	x	x	x			x	x		x	x												
P43	x	x	x		x	x	x	x	x			x										
P44	x	x	x	x			x	x	x							x					x	
P45		x					x															
P46		x	x				x	x		x												
P47	x	x	x			x			x	x												
P48			x				x	x														
P49		x	x				x	x		x												

Appendix A Mapping of Occurrence of Security and Privacy Requirements for WBAN Applications

Ref no	Data Confidentiality	Data Integrity	Authentication	Non-repudiation	Access Control	Availability	Privacy	Encryption/ Cryptography	Key Management	Data Freshness	Firewall	Accountability	Revocability	Intrusion Detection	Trust Management	Forward secrecy / Backward secrecy	Resilience	Physical Protection	Auditability	Client Platform Security	Anonymity	Regulations and compliance requirement
P50	x	x	x		x			x				x							x		x	
P51	x	x	x		x	x	x	x				x	x	x							x	x
P52	x	x	x				x	x														
P53	x	x	x						x													
P54	x		x		x		x	x	x													
P55	x		x														x					
P56	x				x		x	x		x												
P57	x	x	x				x	x	x	x												
P58	x	x	x			x	x	x														
P59	x	x	x				x	x	x													
P60	x	x					x	x														
P61	x	x	x			x		x														
P62	x	x	x	x			x		x							x					x	
P63	x	x	x			x	x	x	x													
P64	x	x					x	x									x				x	
P65	x		x				x	x														
P66	x	x	x		x		x	x													x	
P67	x	x	x		x	x	x	x										x		x		x
P68	x	x	x		x			x	x	x												x
P69		x	x				x			x					x						x	
P70	x	x	x		x		x	x														
P71	x	x	x		x	x		x	x		x						x	x				
P72	x	x	x		x	x	x	x	x	x		x		x	x		x				x	
P73	x	x	x			x	x	x														x
P74	x	x	x		x		x	x	x	x											x	
P75	x	x	x	x	x	x	x	x				x				x					x	x
P76	x	x	x	x	x		x														x	
P77	x	x	x			x		x		x												
P78	x	x	x	x					x							x	x					
P79	x		x	x			x	x	x							x	x				x	
P80	x	x	x										x			x	x					
P81			x				x	x						x								
P82	x	x	x	x			x	x		x					x						x	
P83	x	x	x		x		x	x	x													
P84	x	x	x	x	x		x	x		x		x										
P85	x	x	x			x	x										x					
P86	x	x	x			x	x	x	x							x					x	
P87	x	x	x		x	x	x	x	x	x				x			x					
P88	x	x	x				x	x		x												
P89	x	x			x		x	x	x													
P90	x	x	x			x		x	x	x												
P91	x	x	x		x		x	x	x	x												
P92	x	x	x		x	x	x	x				x										
P93	x	x	x	x	x	x	x	x														
P94	x	x	x	x	x		x					x	x									
P95	x	x	x		x	x		x														
P96	x	x	x		x	x	x	x	x	x					x	x	x				x	x
P97	x	x	x			x	x	x														
P98	x	x	x		x			x		x		x	x									
P99	x	x	x			x			x	x												
P100	x	x	x			x	x	x	x	x												x
P101	x	x	x			x		x	x	x												
P102	x	x	x			x		x	x	x					x		x					
P103			x		x			x														
P104	x	x	x		x	x	x	x	x					x					x			
P105	x	x	x		x	x	x										x					
P106	x	x			x	x	x		x		x	x										
P107	x	x	x	x	x	x	x	x		x		x	x				x		x			
P108	x	x	x				x	x														
P109	x	x	x				x	x	x	x												
P110	x	x	x			x		x	x	x					x		x					

Appendix A Mapping of Occurrence of Security and Privacy Requirements for WBAN Applications

Ref no	Data Confidentiality	Data Integrity	Authentication	Non-repudiation	Access Control	Availability	Privacy	Encryption/ Cryptography	Key Management	Data Freshness	Firewall	Accountability	Revocability	Intrusion Detection	Trust Management	Forward secrecy / Backward secrecy	Resilience	Physical Protection	Auditability	Client Platform Security	Anonymity	Regulations and compliance requirement
P111	x	x	x					x	x													
P112	x	x	x			x	x	x									x					x
P113	x	x	x			x		x														
P114	x	x	x		x		x	x														
P115	x	x				x	x															
P116	x	x	x			x			x													
P117	x	x	x					x														
P118	x	x	x				x	x														
P119	x	x	x				x			x												
P120	x	x	x			x	x									x	x				x	
P121	x	x	x		x		x	x	x										x		x	
P122	x	x	x	x	x	x	x															
P123	x	x	x	x	x	x	x	x		x						x						
P124	x	x	x	x		x	x	x	x	x		x	x									
P125		x	x					x		x												
P126	x	x	x			x	x			x												
P127	x	x	x				x	x									x					
P128	x	x			x		x	x	x									x				x
P129	x	x				x																
P130	x	x	x	x	x	x						x										
P131	x		x		x																	
P132	x	x	x	x				x		x												
P133	x	x	x		x	x		x		x												
P134	x	x				x	x	x							x							
P135	x	x	x			x		x	x	x		x										
P136	x	x	x					x	x	x				x								
P137	x	x	x	x	x	x	x					x	x									x
P138	x	x	x	x		x	x	x	x	x				x								
P139	x	x	x																		x	
P140	x	x	x					x	x													
P141		x	x				x	x	x							x	x					
P142	x	x	x			x		x	x	x												x
P143	x	x	x	x	x	x	x	x					x				x		x		x	
P144	x	x	x				x															
P145	x	x	x	x	x	x	x	x									x	x				
P146	x	x	x		x	x	x	x	x													
P147	x	x	x	x	x	x	x															
P148	x	x	x	x			x	x	x							x					x	
P149		x	x				x	x		x												
P150	x		x				x	x														
P151	x	x	x				x	x	x				x			x					x	
P152		x	x				x	x														
P153	x	x					x	x	x						x							
P154			x				x		x							x					x	
P155	x	x	x				x		x							x						
P156	x	x	x				x	x		x						x		x				
P157			x						x							x					x	
P158	x	x	x		x	x			x	x												
P159	x		x					x														
P160	x	x						x	x													
P161	x		x				x	x													x	
P162			x				x	x	x												x	
P163	x	x					x	x	x										x			
P164		x	x	x			x														x	
P165	x	x	x				x	x	x							x					x	
P166	x	x	x	x		x	x	x	x	x				x			x				x	
P167	x	x	x				x								x							
P168	x		x				x		x												x	
P169		x			x		x	x											x		x	
P170	x	x	x		x	x	x		x							x	x				x	
P171	x	x	x			x		x														

Appendix A Mapping of Occurrence of Security and Privacy Requirements for WBAN Applications

Ref no	**Data Confidentiality**	**Data Integrity**	**Authentication**	**Non-repudiation**	**Access Control**	**Availability**	**Privacy**	**Encryption/ Cryptography**	**Key Management**	**Data Freshness**	**Firewall**	**Accountability**	**Revocability**	**Intrusion Detection**	**Trust Management**	**Forward secrecy / Backward secrecy**	**Resilience**	**Physical Protection**	**Auditability**	**Client Platform Security**	**Anonymity**	**Regulations and compliance requirement**
P172	x	x	x	x												x	x					
P173	x	x	x		x	x	x	x	x					x	x						x	
P174	x	x	x			x		x		x												
P175	x	x	x					x							x							
P176	x	x	x			x	x	x	x	x					x		x					
P177	x	x					x														x	
P178	x	x	x	x								x									x	
P179	x		x				x	x	x												x	
P180	x		x				x	x	x							x					x	
P181	x	x	x		x	x	x	x	x	x						x					x	
P182	x	x	x				x	x	x						x							
P183	x	x					x	x	x													
P184		x	x	x			x	x	x												x	
P185	x	x	x				x			x												
P186	x	x	x		x	x	x	x														
P187	x	x	x			x	x	x	x													
P188			x				x	x	x							x					x	
P189	x	x	x				x	x		x											x	
P190	x	x	x		x	x	x	x		x					x							
P191	x		x						x							x					x	
P192	x	x	x		x	x	x	x														
P193	x	x	x	x	x	x	x	x	x			x	x									
P194	x	x	x			x	x	x	x	x												
P195	x	x	x		x		x	x	x													
P196	x		x		x		x	x														
P197					x		x	x														
P198	x	x	x			x																
P199	x	x	x	x	x	x	x	x						x								
P200	x	x	x				x	x	x			x										
P201	x	x	x			x		x		x		x										
P202	x		x		x		x	x	x													
P203	x	x	x			x	x	x							x							
P204	x	x	x			x	x	x	x	x					x		x					
P205	x	x	x		x	x	x	x	x					x	x							
P206	x	x	x	x		x		x	x	x									x			
P207	x	x	x		x	x	x															

List of selected papers:

P1 Li, M., Lou, W. & Ren, K., 2010. Data security and privacy in wireless body area networks. IEEE Wireless Communications, 17(1), pp.51–58. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5416350%5Cnhttp://apps.webofknowledge.com/full_record.do?product=WOS&search_mode=GeneralSearch&qid=31&SID=P29d2QL6yTZOxYC6ki4&page=1&doc=17.

P2 Saleem, S., Ullah, S. & Kwak, K.S., 2010. Towards security issues and solutions in wireless body area networks. 6th International Conference on Networked Computing (INC), pp.1–4. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5484803.

P3 Partala, J. et al., 2013. Security threats against the transmission chain of a medical health monitoring system. 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom 2013, (Healthcom), pp.243–248.

P4 Omoogun, M. et al., 2017. When eHealth meets the internet of things: Pervasive security and privacy challenges. 2017 International Conference on Cyber Security And Protection Of Digital Services, Cyber Security 2017.

P5 Thamilarasu, G. & Odesile, A., 2016. Securing wireless body area networks: Challenges, review and recommendations. 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1–7. Available at: http://ieeexplore.ieee.org/document/7919700/.

P6 Mainanwal, V., Gupta, M. & Upadhayay, S.K., 2015. A survey on wireless body area network: Security technology and its design methodology issue. 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), (I), pp.1–5. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7193088.

P7 Seneviratne, S. et al., 2017. A survey of wearable devices and challenges. IEEE Communications Surveys and Tutorials, 19(4), pp.2573–2620.

P8 Kompara, M. & Hölbl, M., 2018. Survey on security in intra-body area network communication. Ad Hoc Networks, 70, pp.23–43. Available at: http://www.sciencedirect.com/science/article/pii/S1570870517302068.

P9 Alsadhan, A. & Khan, N., 2013. An LBP based key management for secure wireless body area network (WBAN). 2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp.85–88. Available at: http://ieeexplore.ieee.org/document/6598449/.

P10 Langone, M., Setola, R. & Lopez, J., 2017. Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method. 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), pp.304–309. Available at: http://ieeexplore.ieee.org/document/8029946/.

P11 Al-Janabi, S. et al., 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2), pp.113–122. Available at: http://dx.doi.org/10.1016/j.eij.2016.11.001.

P12 Ramli, S.N. & Ahmad, R., 2011. Surveying the wireless body area network in the realm of wireless communication. 2011 7th International Conference on Information Assurance and Security (IAS), pp.58–61. Available at: http://ieeexplore.ieee.org/document/6122845/.

P13 Naik, M.R.K. & Samundiswary, P., 2016. Wireless body area network security issues — Survey. 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp.190–194. Available at: http://ieeexplore.ieee.org/document/7987943/.

P14 Sawaneh, I.A., Sankoh, I. & Koroma, D.K., 2017. A survey on security issues and wearable sensors in wireless body area network for healthcare system. In Wavelet Active Media Technology and Information Processing (ICCWAMTIP). pp. 304–308.

P15 Dodangeh, P. & Jahangir, A.H., 2018. A biometric security scheme for wireless body area networks. Journal of Information Security and Applications, 41, pp.62–74. Available at: https://doi.org/10.1016/j.jisa.2018.06.001.

P16 Sajid, A. & Abbas, H., 2016. Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of Medical Systems. Available at: http://dx.doi.org/10.1007/s10916-016-0509-2.

P17 Kyaw, A.K. & Cusack, B., 2014. Security challenges in pervasive wireless medical systems and devices. 2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy), HONET-PfE 2014, pp.178–185.

P18 He, D. et al., 2017. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal, 11(4), pp.2590–2601. Available at: http://ieeexplore.ieee.org/document/7458160/.

P19 Cavallari, R. et al., 2014. A survey on wireless body area networks: Technologies and design challenges. IEEE Communications Surveys & Tutorials, PP(99), pp.1–23. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6739368.

P20 Antonescu, B. & Basagni, S., 2013. Wireless body area networks: challenges, trends and emerging technologies. In Proceedings of the 8th international conference on body area networks. pp. 1–7.

P21 Challa, S. et al., 2018. Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions. IEEE Consumer Electronics Magazine, 7(1), pp.57–65.

P22 Singel, D., 2008. A secure cross-layer protocol for multi-hop wireless body area networks. In International Conference on Ad-Hoc Networks and Wireless. pp. 94–107.

P23 Dhillon, P.K. & Kalra, S., 2018. Multi-factor user authentication scheme for IoT-based healthcare services. Journal of Reliable Intelligent Environments. Available at: https://doi.org/10.1007/s40860-018-0062-5.

P24 Jang, C., Lee, D.-G. & Han, J., 2008. A proposal of security framework for wireless body area network. In 2008 International Conference on Security Technology. pp. 202–205. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4725376.

P25 Dharshini, S. & Subashini, M.M., 2017. An overview on wireless body area networks. In Power and Advanced Computing Technologies (i-PACT). pp. 1–10.

P26 Venkatasubramanian, S. & Jothi, V., 2012. Integrated authentication and security check with CDMA modulation technique in physical layer of Wireless Body Area Network. 2012 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2012.

P27 Yin, L. et al., 2017. Security-aware attribute-based access control for fog-based eldercare system. In Computer and Communications (ICCC). pp. 2680–2684.

P28 Li, F. & Hong, J., 2016. Efficient certificateless access control for wireless body area networks. IEEE Sensors Journal, 16(13), pp.5389–5396.

P29 Al Alkeem, E., Yeun, C.Y. & Zemerly, M.J., 2016. Security and privacy framework for ubiquitous healthcare IoT devices. In 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015. pp. 70–75.

P30 Islam, S.M.R. et al., 2015. The internet of things for health care: a comprehensive survey. IEEE Access, 3, pp.678–708. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113786.

P31 Alshamsi, A.Z., Barka, E.S. & Serhani, M.A., 2016. Lightweight encryption algorithm in wireless body area network for e-health monitoring. In 2016 12th International Conference on Innovations in Information Technology (IIT). pp. 1–7. Available at: http://ieeexplore.ieee.org/document/7880042/.

P32 Dimitriou, T. & Ioannis, K., 2008. Security issues in biomedical wireless sensor networks. 2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies, pp.1–5. Available at: http://ieeexplore.ieee.org/document/4712577/.

P33 Sindhu, K. V, 2017. Trustworthy access control for wireless body area networks. In Information Communication and Embedded Systems (ICICES). pp. 1–5.

P34 Ankaralı, Z.E. et al., 2014. A comparative review on the wireless implantable medical devices privacy and security. 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth), pp.246–249.

P35 Fragopoulos, A.G., Gialelis, J. & Serpanos, D., 2010. Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures. 12th IEEE International Conference on e-Health Networking, Application and Services.

P36 Liu, J., 2010. Hybrid security mechanisms for wireless body area networks. In Second International Conference on Ubiquitous and Future Networks (ICUFN). pp. 98–103.

P37 Saleem, K. et al., 2016. Survey on cybersecurity issues in wireless mesh networks based eHealthcare. IEEE 18th International Conference on e-Health Networking, Applications and Services.

P38 Chukwunonyerem, J., Aibinu, A.M. & Onwuka, E.N., 2014. Review on security of wireless body area sensor network. In 11th International Conference on Electronics, Computer and Computation (ICECCO). pp. 1–10. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84921719269&partnerID=tZOtx3y1.

P39 Saarika, U., Sharma, P.K. & Sharma, D., 2016. A roadmap to the realization of wireless body area networks: a review. In International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). pp. 439–443.

P40 Ara, A. et al., 2017. A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. IEEE Access, 5, pp.12601–12617.

P41 Wazid, M. et al., 2017. A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE Journal of Biomedical and Health Informatics, 22(4), pp.1299–1309.

P42 Prakash, S. & Mamta, 2016. An overview of healthcare perspective based security issues in wireless sensor networks. In Comput. for Sustainable Global Development. pp. 870–875.

P43 Alemdar, H. & Ersoy, C., 2010. Wireless sensor networks for healthcare: A survey. Computer Networks, 54(15), pp.2688–2710. Available at: http://www.sciencedirect.com/science/article/pii/S1389128610001398.

P44 Shen, J. et al., 2018. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106(September 2017), pp.117–123. Available at: http://dx.doi.org/10.1016/j.jnca.2018.01.003.

P45 Xu, J. et al., 2018. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. Future Generation Computer Systems. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X17326067.

P46 Javadi, S.S. & Razzaque, M.A., 2013. Security and privacy in wireless body area networks for health care applications. Wireless Networks and Security, 26(3), pp.165–187. Available at: http://link.springer.com/10.1007/978-3-642-36169-2_6.

P47 Ullah, S. & Alamri, A., 2013. A secure RFID-based WBAN for healthcare applications. Journal of medical systems.

P48 Huang, C., Lee, H. & Hoon, D., 2012. A privacy-strengthened scheme for E-healthcare monitoring system. Journal of medical systems, pp.2959–2971.

P49 Ameen, M. Al & Liu, J., 2012. Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, pp.93–101.

P50 Ramu, G., 2018. A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter. Education and Information Technologies.

P51 Saleem, K., Tan, Z. and Buchanan, W. (2017) 'Security for Cyber-Physical Systems in Healthcare', in Thuemmler, C. and Bai, C. (eds) Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare. Cham: Springer International Publishing, pp. 233–251. doi: 10.1007/978-3-319-47617-9_12.

P52 Miao, F. et al. (2009) ‘A novel biometrics based security solution for body sensor networks’, Proceedings of the 2009 2nd International Conference on Biomedical Engineering and Informatics, BMEI 2009. doi: 10.1109/BMEI.2009.5304950.

P53 Muhammad, K. ur R. R. S. et al. (2009) ‘BARI: A Distributed Key Management Approach for Wireless Body Area Networks’, Sensors. IEEE, 10(4), pp. 3911–3933. doi: 10.3390/s100403911.

P54 Zhu, Y. et al. (2009) ‘A lightweight policy system for body sensor networks’, IEEE Transactions on Network and Service Management. IEEE, 6(3), pp. 137–148. doi: 10.1109/TNSM.2009.03.090301.

P55 Amini, S. et al. (2011) ‘Toward a security model for a body sensor platform’, Digest of Technical Papers - IEEE International Conference on Consumer Electronics. IEEE, pp. 143–144. doi: 10.1109/ICCE.2011.5722507.

P56 Zhu, Y. et al. (2012) ‘Vesta: A secure and autonomic system for pervasive healthcare’. doi: 10.4108/icst.pervasivehealth2009.5939.

P57 Kumar, P., Lee, S. G. and Lee, H. J. (2011) ‘A user authentication for healthcare application using wireless medical sensor networks’, Proc.- 2011 IEEE International Conference on HPCC 2011 - 2011 IEEE International Workshop on FTDCS 2011 -Workshops of the 2011 Int. Conf. on UIC 2011- Workshops of the 2011 Int. Conf. ATC 2011. IEEE, 1, pp. 647–652. doi: 10.1109/HPCC.2011.92.

P58 Hosseini-Khayat, S. (2011) ‘A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices’, 2011 5th International Symposium on Medical Information and Communication Technology, ISMICT 2011. IEEE, pp. 6–9. doi: 10.1109/ISMICT.2011.5759785.

P59 Khalil, B. and Naja, N. (2019) ‘A Framework for Security Analytics of WBAN/WLAN Healthcare Network’, 2018 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2018. IEEE, pp. 314–319. doi: 10.1109/ITMC.2018.8691294.

P60 Mekki, N. et al. (2018) ‘A Privacy-Preserving Scheme Using Chaos Theory for Wireless Body Area Network’, 2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018. IEEE, pp. 774–779. doi: 10.1109/IWCMC.2018.8450293.

P61 Chowdhury, F. S. et al. (2018) ‘An implementation of a lightweight end-to-end secured communication system for patient monitoring system’, 2018 Emerging Trends in Electronic Devices and Computational Techniques, EDCT 2018. IEEE, pp. 1–5. doi: 10.1109/EDCT.2018.8405076.

P62 Guan, T., Gui, Z. and Ji, S. (2018) ‘Anonymous and certificateless remote data communication protocol for WBANs’, Proceedings - 2018 1st International Cognitive Cities Conference, IC3 2018. IEEE, pp. 154–159. doi: 10.1109/IC3.2018.00-39.

P63 Usman, M. et al. (2018) ‘Security in wireless body area networks: From in-body to off-body communications’, IEEE Access. IEEE, 6, pp. 58064–58074. doi: 10.1109/ACCESS.2018.2873825.

P64 Arfaoui, A. et al. (2019) 'Context-aware access control and anonymous authentication in WBAN', Computers and Security. Elsevier Ltd, (xxxx). doi: 10.1016/j.cose.2019.03.017.

P65 Wang, G., Lu, R. and Guan, Y. L. (2019) 'Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System', IEEE Access. IEEE, 7, pp. 33565–33576. doi: 10.1109/ACCESS.2019.2891775.

P66 Wang, X. and Jin, Z. (2019) 'An Overview of Mobile Cloud Computing for Pervasive Healthcare', IEEE Access. IEEE, 7, pp. 66774–66791. doi: 10.1109/ACCESS.2019.2917701.

P67 Yaqoob, T., Abbas, H. and Atiquzzaman, M. (2019) 'Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices − A Review', IEEE Communications Surveys and Tutorials. doi: 10.1109/COMST.2019.2914094.

P68 Networks (2018) 'ECG-Based Secure Healthcare Monitoring System in Body Area Networks', 2018 Fourth International Conference on Biosignals, Images and Instrumentation (ICBSII). IEEE, 16(2), pp. 171–193. Available at: https://www.cst.com/Content/Events/downloads/euc2013/3-1-4_CST_EUC.pdf.

P69 Kale, S. S. and Bhagwat, D. S. (2018) 'A Secured IoT Based Webcare Healthcare Controlling System using BSN', in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, pp. 816–821.

P70 Jiang, W., Tan, J. and Liu, W. (2019) 'An Internal Node Reprogrammable Security Scheme Based on IEEE 802.15.6 in Wireless Body Area Networks', pp. 285–289. doi: 10.1145/3291842.3291862.

P71 Sundararajan, A., Sarwat, A. I. and Pons, A. (2019) 'A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems', ACM Computing Surveys, 52(2), pp. 1–36. doi: 10.1145/3309550.

P72 Yaseen, M. et al. (2018) 'Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art', Telematics and Informatics. Elsevier, 35(4), pp. 702–726. doi: 10.1016/j.tele.2017.08.005.

P73 Aceto, G., Persico, V. and Pescapé, A. (2018) 'The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges', Journal of Network and Computer Applications. Elsevier, 107(July 2017), pp. 125–154. doi: 10.1016/j.jnca.2018.02.008.

P74 Dhanvijay, M. M. and Patil, S. C. (2019) 'Internet of Things: A survey of enabling technologies in healthcare and its applications', Computer Networks. Elsevier B.V., 153, pp. 113–131. doi: 10.1016/j.comnet.2019.03.006.

P75 Pramanik, P. K. D., Pareek, G. and Nayyar, A. (2019) Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards, Telemedicine Technologies. Elsevier Inc. doi: 10.1016/b978-0-12-816948-3.00014-3.

P76 Li, Z. and Zhou, Y. (2018) 'Secure and achievable heterogeneous access control scheme for wireless body area networks', Communications in Computer and Information Science, 879, pp. 190–198. doi: 10.1007/978-981-13-3095-7_15.

P77 Saif, S., Gupta, R. and Biswas, S. (2018) 'Implementation of Cloud-Assisted Secure Data Transmission in WBAN for Healthcare Monitoring', in Bhattacharyya, S. et al. (eds) Advanced Computational and Communication Paradigms. Singapore: Springer Singapore, pp. 665–674.

P78 Liu, X., Jin, C. and Li, F. (2018) ‘An Improved Two-Layer Authentication Scheme for Wireless Body Area Networks’, Journal of Medical Systems. Journal of Medical Systems, 42(8). doi: 10.1007/s10916-018-0990-x.

P79 Li, X. et al. (2018) ‘Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors’, Telecommunication Systems. Springer US, 67(2), pp. 323–348. doi: 10.1007/s11235-017-0340-1.

P80 Shen, Jian, Chang, S., et al. (2018) ‘Implicit authentication protocol and self-healing key management for WBANs’, Multimedia Tools and Applications. Multimedia Tools and Applications, pp. 1–21. doi: 10.1007/s11042-017-5559-z.

P81 Anguraj, D. K. and Smys, S. (2019) ‘Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks’, Wireless Personal Communications. Springer US, 104(1), pp. 1–20. doi: 10.1007/s11277-018-6005-x.

P82 Siva Bharathi, K. R. and Venkateswari, R. (2019) ‘Security Challenges and Solutions for Wireless Body Area Networks’, in Comp., Comm.. and Signal Proc., pp. 275–283.

P83 Kołodziej, J. et al. (2019) ‘Ultra Wide Band Body Area Networks: Design and Integration with Computational Clouds’, in Kołodziej, J. and González-Vélez, H. (eds) High-Performance Modelling and Simulation for Big Data Applications: Selected Results of the COST Action IC1406 cHiPSet. Cham: Springer International Publishing, pp. 279–306. doi: 10.1007/978-3-030-16272-6_10.

P84 Punj, R. and Kumar, R. (2019) Technological aspects of WBANs for health monitoring: a comprehensive review, Wireless Networks. Springer US. doi: 10.1007/s11276-018-1694-3.

P85 Shah, S. T. U. et al. (2018) 'Internet of Things-Based Healthcare: Recent Advances and Challenges', pp. 153–162. doi: 10.1007/978-3-319-96139-2_15.

P86 Sharma, G. and Kalra, S. (2018) 'A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services', Iranian Journal of Science and Technology, Transactions of Electrical Engineering. Springer International Publishing, 5. doi: 10.1007/s40998-018-0146-5.

P87 Saleem (2009) 'On the Security Issues in Wireless Body Area Networks', International Journal of Digital Content Technology and its Applications, 3(3). doi: 10.4156/jdcta.vol3.issue3.22.

P88 Dave, S. et al. (2010) 'A secure low-delay protocol for wireless body area networks', 2, pp. 53–72.

P89 Santra, T. (2010) 'Mobile Health Care System for Patient Monitoring', Communications in Computer and Information Science, 101, pp. 695–700. doi: 10.1007/978-3-642-15766-0_123.

P90 Saleem, S., Ullah, S. and Kwak, K. S. (2011) 'A study of IEEE 802.15.4 security framework for wireless body area networks', Sensors, 11(2), pp. 1383–1395. doi: 10.3390/s110201383.

P91 Latré, B. et al. (2011) 'A survey on wireless body area networks', Wireless Networks, 17(1), pp. 1–18. doi: 10.1007/s11276-010-0252-4.

P92 Darwish, A. and Hassanien, A. E. (2011) 'Wearable and implantable wireless sensor network solutions for healthcare monitoring', Sensors, 11(6), pp. 5561–5595. doi: 10.3390/s110605561.

P93 Jang, C. S. et al. (2011) 'Hybrid security protocol for wireless body area networks', Wireless Communications and Mobile Computing. Wiley Online Library, 11(2), pp. 277–288.

P94 Bradai, N., Chaari, L. and Kamoun, L. (2011) 'A Comprehensive Overview of Wireless Body Area Networks (WBAN)', International Journal of E-Health and Medical Communications, 2(3), pp. 1–30. doi: 10.4018/jehmc.2011070101.

P95 Anand, S. (2011) 'Security architecture for at-home medical care using body sensor network', Int. J. Ad-hoc, Sensor, Ubiquitous Comput, 2(1), pp. 60–69.

P96 Kumar, P. and Lee, H. J. (2012) 'Security issues in healthcare applications using wireless medical sensor networks: A survey', Sensors, 12(1), pp. 55–91. doi: 10.3390/s120100055.

P97 V. Crosby, G. (2012) 'Wireless Body Area Networks for Healthcare: A Survey', International Journal of Ad hoc, Sensor & Ubiquitous Computing, 3(3), pp. 1–26. doi: 10.5121/ijasuc.2012.3301.

P98 Ragesh, G. K. and Baskaran, K. (2013) 'Addressing the Need for Context Awareness and Security Requirements in Wireless Body Area Networks', International Journal of Future Computer and Communication, 1(3), pp. 302–305. doi: 10.7763/ijfcc.2012.v1.81.

P99 T.MeenaAbarna, K. and Venkatachalapathy, K. (2012) 'Light-weight Security Architecture for IEEE 802. 15. 4 Body Area Networks', International Journal of Computer Applications, 47(22), pp. 1–8. doi: 10.5120/7485-9972.

P100 Qadri, S. F. et al. (2013) 'Applications, challenges, security of wireless body area networks (WBANs) and functionality of IEEE 802.15. 4/ZIGBEE', Science International Lahore, 25(4), pp. 697–702.

P101 Fatema, N. and Brad, R. (2014) 'Security Requirements, Counterattacks and Projects in Healthcare Applications Using WSNs - A Review', 2(2), pp. 1–9. Available at: http://arxiv.org/abs/1406.1795.

P102 Pathania, S. and Bilandi, N. (2014) 'Security Issues in Wireless Body Area Network', International Journal of Computer Science and Mobile Computing, 3(4), pp. 1171–1178.

P103 Lee, Y. S., Alasaarela, E. and Lee, H. (2014) 'Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system', International Conference on Information Networking. IEEE, pp. 453–457. doi: 10.1109/ICOIN.2014.6799723.

P104 Kang, J. and Adibi, S. (2015) 'A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN)', in Doss, R., Piramuthu, S., and ZHOU, W. (eds) Future Network Systems and Security. Cham: Springer International Publishing, pp. 61–83.

P105 Picazo-Sanchez, P. et al. (2014) 'Secure publish-subscribe protocols for heterogeneous medical wireless body area networks', Sensors (Switzerland), 14(12), pp. 22619–22642. doi: 10.3390/s141222619.

P106 Wang, J. et al. (2013) 'A research on security and privacy issues for patient related data in medical organization system', International Journal of Security and its Applications, 7(4), pp. 287–298.

P107 Sawand, A. et al. (2015) 'Toward energy-efficient and trustworthy eHealth monitoring system', China Communications, 12(1), pp. 46–65. doi: 10.1109/CC.2015.7084383.

P108 MurtazaRashidAlMasud, S. (2013) ‘Study and Analysis of Scientific Scopes, Issues and Challenges towards Developing a Righteous Wireless Body Area Network’, International Journal of Computer Applications, 74(6), pp. 46–56. doi: 10.5120/12893-0061.

P109 Sangari, S. and Manickam, M. (2014) ‘Security and Privacy in Wireless Body Area Network’, Indian Streams Research Journal, 5(8), pp. 1–7. doi: 10.9780/22307850.

P110 Niksaz, P. (2015) ‘Wireless Body Area Networks: Attacks and Countermeasures’, International Journal of Scientific & Engineering Research, 6(9), pp. 556–568. Available at: http://www.ijser.org.

P111 Tote, S. S., Khupse, S. M. and Bhutwani, K. S. (2015) ‘Data Authentication in Wireless Body Area Network (WBAN) Using A Biometric-Based Security’, International Journal for Research in Emerging Science and Technology, 2(1), pp. 136–142.

P112 Huang, R. (2015) ‘Prospect of Wireless Body Area Network Technology’, (Esac), pp. 246–249. doi: 10.2991/esac-15.2015.61.

P113 Kaur, M. (2015) ‘A Study on Networking Techniques of WBAN System’.

P114 Saha, M. S. and Anvekar, D. K. (2014) ‘State of The Art in WBAN Security & Open Research Issues’, (July).

P115 Karande, S. N. and Lohiya, G. B. (2015) ‘Trustworthiness of Wireless Body Area Networks (WBANs) and Medical Devices in Healthcare Applications’, 4(3), pp. 497–503.

P116 Minocha, S. (2013) ‘WBAN and its Applications’, International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS), 02(01), pp. 11–14.

P117 Al-Janabi, S., Dawood, A. and Salman, A. (2013) 'Distributed Data Security and Privacy in WBAN-Related e-Health Systems', AL-Mansour Journal, (20), pp. 121–132.

P118 Soh, P. J. et al. (2015) 'Wearable wireless health monitoring: Current developments, challenges, and future trends', IEEE Microwave Magazine, 16(4), pp. 55–70. doi: 10.1109/MMM.2015.2394021.

P119 Tayal, A. and Prachi (2013) 'Securing E-healthcare applications with PPS and PDS', International Conference on Advanced Computing and Communication Technologies, ACCT. IEEE, pp. 45–49. doi: 10.1109/ACCT.2013.20.

P120 Ibrahim, M. H. et al. (2016) 'Secure anonymous mutual authentication for star two-tier wireless body area networks', Computer Methods and Programs in Biomedicine. Elsevier Ireland Ltd, 135(July), pp. 37–50. doi: 10.1016/j.cmpb.2016.07.022.

P121 Sun, W. et al. (2018) 'Security and Privacy in the Medical Internet of Things: A Review', Security and Communication Networks, 2018, pp. 1–9. doi: 10.1155/2018/5978636.

P122 Liu, X. et al. (2016) 'A secure medical information management system for wireless body area networks', KSII Transactions on Internet and Information Systems, 10(1), pp. 221–237. doi: 10.3837/tiis.2016.01.013.

P123 Fotouhi, H. et al. (2016) 'Communication and Security in Health Monitoring Systems - A Review', Proceedings - International Computer Software and Applications Conference. IEEE, 1, pp. 545–554. doi: 10.1109/COMPSAC.2016.8.

P124 Khernane, N., Potop-Butucaru, M. and Chaudet, C. (2017) 'BANZKP: A Secure Authentication Scheme Using Zero Knowledge Proof for WBANs', Proceedings - 2016 IEEE

13th International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2016. IEEE, pp. 307–315. doi: 10.1109/MASS.2016.046.

P125 Khan, R. A. (2018) ‘The state-of-the-art wireless body area sensor networks : A survey’, 14(1204). doi: 10.1177/1550147718768994.

P126 Kanjee, M. R. and Liu, H. (2016) ‘Authentication and key relay in medical cyber-physical systems’, Security and Communication Networks, pp. 874–885. doi: 10.1002/sec.1009.

P127 Boulemtafes, A. and Badache, N. (2016) ‘Wearable Health Monitoring Systems: An Overview of Design Research Areas’, 20, pp. 17–27. doi: 10.1007/978-3-319-23341-3.

P128 Abdullah, A. H. et al. (2018) ‘Securing Data Communication in Wireless Body Area Networks Using Digital Signatures’, Technical Journal, 23(02), pp. 50–55. Available at: http://tj.uettaxila.edu.pk/index.php/technical-journal/article/view/757.

P129 N., S. and H., R. (2016) ‘Recent Research on Wireless Body Area Networks: A Survey’, International Journal of Computer Applications, 142(11), pp. 42–48. doi: 10.5120/ijca2016909893.

P130 Mapoka, T. et al. (2018) ‘Secure Mutual Self-Authenticable Mechanism for Wearable Devices’, International Journal for Information Security Research, 6(1), pp. 625–635. doi: 10.20533/ijisr.2042.4639.2016.0072.

P131 Karmakar, K. et al. (2018) ‘WBAN Security: Study and implementation of a biological key based framework’, Proceedings of 5th International Conference on Emerging Applications of Information Technology, EAIT 2018. IEEE, pp. 1–6. doi: 10.1109/EAIT.2018.84704095.

P132 Tariq, M. (2017) ‘Threats, Challenges, Security of Wire Less Body Area Networks (Wban) Using Ieee 802.15.4/Zigbee’, International Journal of Scientific & Engineering Research, 8(5). Available at: http://www.ijser.org.

P133 Muka, R., Yildrim-Yayilgan, S. and Sevrani, K. (2019) ‘Security Analysis of Wireless BAN in e-Health’, International Journal of Business & Technology, 5(2), pp. 1–7. doi: 10.33107/ijbte.2017.5.2.02.

P134 Lofty, A. N. (no date) ‘Fundamental Security Challenges in Internet of Things Healthcare Services’, pp. 1–6.

P135 Kamoona, M. A. and Azzazi, A. (2018) ‘Importance of WBAN and Its Security : An Overview’, (8), pp. 30–34.

P136 Ren, Y. et al. (2019) ‘Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network’, Sensors, 19(10), p. 2395. doi: 10.3390/s19102395.

P137 Bahena, K. and Tu, M. (2016) ‘WBAN Security Management in Healthcare Enterprise Environments’, Annual ADFSL Conference on Digital Forensics, Security and Law, (4).

P138 Taha, M. S. et al. (2018) ‘Wireless Body Area Network revisited’, International Journal of Engineering & Technology, 7(4), pp. 35–46. doi: 10.15446/rsap.v18n6.517945.

P139 Izza, S., Benssalah, M. and Ouchikh, R. (2019) ‘Security Improvement of the Enhanced 1-round Authentication Protocol for Wireless Body Area Networks’, Proceedings of the 2018 International Conference on Applied Smart Systems, ICASS 2018. IEEE, (November), pp. 1–6. doi: 10.1109/ICASS.2018.8652036.

P140 Saif, S. and Biswas, S. (2019) Secure Data Transmission Beyond Tier 1 of Medical Body Sensor Network. Springer Singapore. doi: 10.1007/978-981-13-1544-2.

P141 Hathaliya, J. J. et al. (2019) 'Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach', Computers and Electrical Engineering. Elsevier Ltd, 76, pp. 398–410. doi: 10.1016/j.compeleceng.2019.04.0175.

P142 Karthikeyan, M. V. and Martin Leo Manickam, J. (2016) 'Security issues in wireless body area networks: In bio-signal input fuzzy security model: A survey', Research Journal of Pharmaceutical, Biological and Chemical Sciences, 7(6), pp. 1755–1773.

P143 Masood, I. et al. (2018) 'Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure', Wireless Communications and Mobile Computing, 2018, pp. 1–23. doi: 10.1155/2018/2143897.

P144 Bouazizi, A. et al. (2017) 'Wireless body area network for e-health applications: Overview', in Int. Conf. on SM2C, pp. 17–19.

P145 Prema, L. and Devi, L. (2017) 'An Efficient Authentication & Light Weight Security in WBAN', International Journal of Engineering Science and Computing, 7(11), pp. 15679–15683. Available at: http://ijesc.org/.

P146 Olakanmi, O. O. (2017) 'Lightweight Security and Privacy Scheme for Wireless Body Area Network in E-Health System', International Journal of Information Security Science, 6(3), pp. 26–38. Available at: https://www.semanticscholar.org/paper/Lightweight-Security-and-Privacy-Scheme-for-Body-in-Olakanmi/b34866031740e5249fb54d673ce3869eac5600b6.

P147 Zou, S. et al. (2017) 'A Survey on Secure Wireless Body Area Networks', Security and Communication Networks, 2017. doi: 10.1155/2017/3721234.

P148 Li, T., Zheng, Y. and Zhou, T. (2017) 'Efficient Anonymous Authenticated Key Agreement Scheme for Wireless Body Area Networks', Security and Communication Networks, 2017. doi: 10.1155/2017/4167549.

P149 Jeedella, J. S. Y. and Al-Qutayri, M. (2017) 'Technological Solutions for Smart Homes', in van Hoof, J., Demiris, G., and Wouters, E. J. M. (eds) Handbook of Smart Homes, Health Care and Well-Being. Cham: Springer International Publishing, pp. 1–13. doi: 10.1007/978-3-319-01904-8_47-1.

P150 Umar, M., Wu, Z. and Liao, X. (2020) 'Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics', *IEEE Access*. IEEE, 8, pp. 66411–66422. doi: 10.1109/ACCESS.2020.2985261.

P151 Kumar, M. and Chand, S. (2020) 'A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network', *IEEE Systems Journal*, 15(2), pp. 2779–2786. doi: 10.1109/jsyst.2020.2990749.

P152 Chen, H. *et al.* (2020) 'Security design of ECG telemonitoring systems', *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020*, pp. 707–711. doi: 10.1109/ICCEA50009.2020.00154.

P153 Mehmood, G. *et al.* (2020) 'A Trust-Based Energy-Efficient and Reliable Communication Scheme (Trust-Based ERCS) for Remote Patient Monitoring in Wireless Body Area Networks', *IEEE Access*, 8, pp. 131397–131413. doi: 10.1109/ACCESS.2020.3007405.

P154 Feng, Q. *et al.* (2019) 'Lightweight collaborative authentication with key protection for smart electronic health record system', *IEEE Sensors Journal*. IEEE, 20(4), pp. 2181–2196.

P155 Yang, X. *et al.* (2021) 'Efficient and Anonymous Authentication for Healthcare Service with Cloud based WBANs', *IEEE Transactions on Services Computing,* 00(00). doi: 10.1109/TSC.2021.3059856.

P156 Hariharan, U., Rajkumar, K. and Ponmalar, A. (2021) 'WBAN for e-Healthcare Application: Systematic Review, Challenges, and Counter Measures', in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–7.

P157 Xu, Z. *et al.* (2019) 'A lightweight mutual authentication and key agreement scheme for medical internet of things', *IEEE Access*. IEEE, 7, pp. 53922–53931. doi: 10.1109/ACCESS.2019.2912870.

P158 Mucchi, L. *et al.* (2019) 'An Overview of Security Threats, Solutions and Challenges in WBANs for Healthcare', *International Symposium on Medical Information and Communication Technology, ISMICT*. IEEE, 2019-May, pp. 4–9. doi: 10.1109/ISMICT.2019.8743798.

P159 Umar, M., Liao, X. and Chen, J. (2019) 'Enhanced BAN-GZKP: Optimal zero knowledge proof based scheme in body area networks', *Proceedings - 2019 International Conference on Networking and Network Applications, NaNA 2019*. IEEE, pp. 96–101. doi: 10.1109/NaNA.2019.00026.

P160 iang, Q. *et al.* (2019) 'Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network', *IEEE Transactions on Emerging Topics in Computing*. IEEE, 9(2), pp. 839–853. doi: 10.1109/TETC.2019.2949137.

P161 Altaf, F. *et al.* (2019) 'Privacy preserving lightweight searchable encryption for cloud assisted e-health system', *2019 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2019*. IEEE, pp. 310–314. doi: 10.1109/WiSPNET45539.2019.9032730.

P162 Sahoo, S. S. and Mohanty, S. (2019) 'Chaotic Map based Privacy Preservation User Authentication Scheme for WBANs', *IEEE Region 10 Annual International Conference, Proceedings/TENCON*. IEEE, 2019-Octob, pp. 1037–1042. doi: 10.1109/TENCON.2019.8929338.

P163 Zhang, X. *et al.* (2019) 'CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors', *IEEE Transactions on Cloud Computing*. IEEE.

P164 Liu, X., Zhang, R. and Zhao, M. (2019) 'A robust authentication scheme with dynamic password for wireless body area networks', *Computer Networks*. Elsevier, 161, pp. 220–234.

P165 Kompara, M., Islam, S. H. and Hölbl, M. (2019) 'A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs', *Computer Networks*. Elsevier B.V., 148, pp. 196–213. doi: 10.1016/j.comnet.2018.11.016.

P166 Hussain, M. *et al.* (2019) 'Authentication techniques and methodologies used in wireless body area networks', *Journal of Systems Architecture*. Elsevier, 101, p. 101655.

P167 Hasan, K. *et al.* (2019) 'A comprehensive review of wireless body area network', *Journal of Network and Computer Applications*. Elsevier, 143, pp. 178–198.

P168 Shuai, M. *et al.* (2020) 'Efficient and privacy-preserving authentication scheme for wireless body area networks', *Journal of Information Security and Applications*. Elsevier, 52, p. 102499.

P169 Ray, P. P., Dash, D. and Kumar, N. (2020) 'Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions', *Computer Communications*. Elsevier, 160, pp. 111–131.

P170 Hathaliya, J. J. and Tanwar, S. (2020) 'An exhaustive survey on security and privacy issues in Healthcare 4.0', *Computer Communications*. Elsevier, 153, pp. 311–335.

P171 Arya, K. V and Gore, R. (2020) 'Data security for WBAN in e-health IoT applications', in *Intelligent data security solutions for e-health applications*. Elsevier, pp. 205–218.

P172 Ullah, I. *et al.* (2021) 'Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN)', *Microprocessors and Microsystems*. Elsevier, 81, p. 103477.

P173 Aman, A. H. M. *et al.* (2021) 'IoMT amid COVID-19 pandemic: Application, architecture, technology, and security', *Journal of Network and Computer Applications*. Elsevier, 174, p. 102886.

P174 Hajar, M. S., Al-Kadri, M. O. and Kalutarage, H. K. (2021) 'A survey on wireless body area networks: Architecture, security challenges and research opportunities', *Computers \& Security*. Elsevier, 104, p. 102211.

P175 Sudha, R. (2021) 'An Emerging Trust-Based Security on Wireless Body Area Network', in *Sustainable Communication Networks and Application*. Springer, pp. 215–226.

P176 Roy, M., Chowdhury, C. and Aslam, N. (2020) ‘Security and privacy issues in wireless sensor and body area networks’, in *Handbook of computer networks and cyber security*. Springer, pp. 173–200.

P177 Singh, R. *et al.* (2020) ‘Wireless body area network: An application of IoT and its issuses—A survey’, in *Computational Intelligence in Pattern Recognition*. Springer, pp. 285–293.

P178 Kasyoka, P., Kimwele, M. and Angolo, S. M. (2020) ‘Towards an efficient certificateless access control scheme for wireless body area networks’, *Wireless Personal Communications*. Springer, 115(2), pp. 1257–1275.

P179 Song, Y. and Tan, H. (2020) ‘Practical pairing-Free sensor cooperation scheme for cloud-Assisted wireless body area networks’, *Cybersecurity*. SpringerOpen, 3(1), pp. 1–9.

P180 Narwal, B. and Mohapatra, A. K. (2020) ‘SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks’, *Wireless Personal Communications*. Springer, 113(4), pp. 1985–2008.

P181 Chatterjee, K. (2020) ‘An improved authentication protocol for wireless body sensor networks applied in healthcare applications’, *Wireless Personal Communications*. Springer, 111(4), pp. 2605–2623.

P182 Vyas, A. and Pal, S. (2020) ‘Preventing security and privacy attacks in WBANs’, in *Handbook of computer networks and cyber security*. Springer, pp. 201–225.

P183 Sharmila, A. H. and Jaisankar, N. (2020) ‘E-MHMS: enhanced MAC-based secure delay-aware healthcare monitoring system in WBAN’, *Cluster Computing*. Springer, 23(3), pp. 1725–1740.

P184 Mwitende, G. *et al.* (2020) ‘Authenticated key agreement for blockchain-based WBAN’, *Telecommunication Systems*. Springer, 74(3), pp. 347–365.

P185 Dhaya, R., Kanthavel, R. and Algarni, F. (2020) 'Research perspectives on applications of internet-of-things technology in healthcare WIBSN (wearable and implantable body sensor network)', *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Springer, pp. 279–304.

P186 Jimenez, J. I., Jahankhani, H. and Kendzierskyj, S. (2020) 'Health care in the cyberspace: Medical cyber-physical system and digital twin challenges', in *Digital twin technologies and smart cities*. Springer, pp. 79–92.

P187 Kang, J. J. (2020) 'Systematic analysis of security implementation for internet of health things in mobile health networks', in *Data Science in Cybersecurity and Cyberthreat Intelligence*. Springer, pp. 87–113.

P188 Sowjanya, K., Dasgupta, M. and Ray, S. (2020) 'An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems', *International Journal of Information Security*. Springer, 19(1), pp. 129–146.

P189 Aileni, R. M. *et al.* (2020) 'Data privacy and security for IoMWT (internet of medical wearable things) cloud', in *IoT and ICT for Healthcare Applications*. Springer, pp. 191–215.

P190 Raju, M. H. *et al.* (2020) 'Security analysis and a potential layer to layer security solution of medical cyber-physical systems', in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Springer, pp. 61–86.

P191 Xu, J. *et al.* (2019) 'A hybrid mutual authentication scheme based on blockchain technology for WBANs', in *International Conference on Blockchain and Trustworthy Systems*, pp. 350–362.

P192 Nidhya, R. and Karthik, S. (2019) 'Security and privacy issues in remote healthcare systems using wireless body area networks', in *Body Area Network Challenges and Solutions*. Springer, pp. 37–53.

P193 Kumar, D. *et al.* (2019) 'General Outlook of Wireless Body Area Sensor Networks', in *International Conference on Advances in Computing and Data Sciences,* pp. 58–67.

P194 Kumar Panigrahy, S. *et al.* (2019) 'Comparative study of ECG-based key agreement schemes in wireless body sensor networks', in *Recent findings in intelligent computing techniques*. Springer, pp. 151–161.

P195 Blasco, J. *et al.* (2019) 'Wearables security and privacy', in *Mission-Oriented Sensor Networks and Systems: Art and Science*. Springer, pp. 351–380.

P196 Hong, J. *et al.* (2019) 'A combined public-key scheme in the case of attribute-based for wireless body area networks', *Wireless Networks*. Springer US, 25(2), pp. 845–859. doi: 10.1007/s11276-017-1597-8.

P197 Vaniprabha, A. and Poongodi, P. (2019) 'Augmented lightweight security scheme with access control model for wireless medical sensor networks', *Cluster Computing*. Springer, 22(5), pp. 12495–12505.

P198 Hussain, A. *et al.* (2021) 'Security framework for IoT based real-time health applications', *Electronics*. MDPI, 10(6), p. 719.

P199 Hameed, S. S. *et al.* (2021) 'A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches', *PeerJ Computer Science*. PeerJ Inc., 7, p. e414.

P200 Guglielmi, A. V *et al.* (2021) 'Information theoretic key agreement protocol based on ECG signals', in *2021 IEEE Global Communications Conference (GLOBECOM),* pp. 1–6.

P201 Sultana, S. *et al.* (2020) ‘A Critical Study on Internet of Medical Things for Secure WBAN’, in *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*. IGI Global, pp. 179–197.

P202 Paramita, S. (2020) ‘IoT-Based WBAN Health Monitoring System with Security’, in *Internet of Things*. CRC Press, pp. 107–120.

P203 Al Hayajneh, A. *et al.* (2020) ‘Security of broadcast authentication for cloud-enabled wireless medical sensor devices in 5G networks’, *Computer and Information Science*. Canadian Center of Science and Education, 13(2), pp. 1–13.

P204 Raza, A. *et al.* (2020) ‘Comprehensive survey of routing protocols for wireless body area networks (WBANs)’, *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*. IGI Global, pp. 145–178.

P205 Obaidat, M. A. *et al.* (2020) ‘A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures’, *Computers*. MDPI, 9(2), p. 44.

P206 Manju, M. and others (2020) ‘Improved Audit-based malevolent Node Detection and Energy Efficiency for Healthcare Applications.’, *Indian Journal of Public Health Research \& Development*, 11(6).

P207 Asam, M. *et al.* (2019) ‘Security Issues in WBANs’, *arXiv preprint arXiv:1911.04330*.

Appendix B Structure of WBANSecRM Beta Version

How to use the framework

This framework is designed with a progressive logic to align with the software development lifecycle. While using this document, it is recommended to start from the beginning and follow the step-by-step process. The outcome from each step will be used as input from the next step. The user is advised to create the initial product requirements before start using this framework. Once the initial product requirements are finalised, the first step is to set up the scope of the application, followed by conducting the risk analysis in the requirement analysis phase and system architecture phase. The outcome of the risk analysis in both stages will help identify the required control to implement for mitigating the risk. The select control will then be implemented during the implementation phase, followed by testing the efficacy in the testing phase of the software development lifecycle. Furthermore, a case study example is added in the appendix to assist the user in implementing the framework.

1 Executive Summary

A Wireless Body Area Network (WBAN) application is composed of intelligent, low-power sensor nodes which monitor body functions and physiological states. These sensor nodes can collect and process data, store it locally and transmit it to an actuator or a local server for further processing. WBAN applications are gaining popularity in both medical and non-medical domains due to recent advances in sensor technology, integrated circuits, and wireless communication. Both types of application (i.e. medical and non-medical) collect personal health record (PHR) data to provide real-time healthcare monitoring services. Due to the advancement of sensor and wireless communication technology and the increasing popularity of healthcare-based applications, this sector is becoming one of the primary targets for security breaches and cyber threats. A WBAN security breach not only costs money, it can create a life-threatening event. Therefore, security and privacy safeguards need to be considered during the development of this type of healthcare application. Additionally, assuring security and privacy is a key requirement of compliance with legislation and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

Assuring data security and privacy of PHR data in a WBAN application is a key challenge for an organisation and its developers. Most developers have limited knowledge of market-specific regulatory requirements and security standards. Usually, these security standards consist of a vast number of security controls which have insufficient implementation detail. Additionally, implementing security controls for sensor device nodes is complex. Device nodes are often limited by physical memory constraints, computational power and storage. This makes it difficult for a developer to select and prioritise the appropriate controls without compromising the product delivery plan. The purpose of this data security framework is to assist WBAN developers and organisations in assuring the security and privacy of the PHR in a regulatory compliance manner.

2 Scope

Developing a WBAN based healthcare application and managing software development activities throughout the software development lifecycle (SDLC) is a challenging task. ISO 62304 - Medical Device software - software lifecycle processes (IEC 62304, 2019) is a widely known standard which provides guidelines for each stage of the medical device software lifecycle with activities and tasks required for the safe design and maintenance of medical device software. This standard is recognized by the FDA, EU and other regulatory agencies across the world. IEC 62304 recommends that organisations establish and maintain a risk management process to manage risk associated with security. The process should provide a methodology to identify the vulnerabilities, evaluate the associated threats, and implement risk controls to mitigate these threats. Finally, the process should also monitor the effectiveness of the risk control. ISO 62304 also refers to the ISO 14971 - *Medical devices - Application of risk management to medical devices* (BSI, 2009) standard for safety and the AAMI TIR 57 - *Principles for medical device security—Risk management* (AAMI TIR57, 2016) provides guidelines for security related risk management. The framework presented in this document provides guidance for assuring data security and privacy for a WBAN application within the information security and privacy risk management framework defined by AAMI TIR 57. This guidance is intended to assist organisations of any size (small, medium and large) to develop WBAN applications by:

1) Identifying threats, vulnerabilities, and assets associated with WBAN applications
2) Estimating and evaluating associated security and privacy risks
3) Implementing security and privacy risk controls
4) Monitoring the effectiveness of the security and privacy risk controls

The safety risk management and post-production activities is set out of the scope while developing the framework.

3 Overview

A key goal of this data security and privacy framework (presented in Figure Appendix B- 1 overleaf) is to assure the security and privacy of WBAN applications; therefore, the risk management process presented in this framework is based on the TIR 57 risk management process. The TIR 57 risk management process contains six stages:

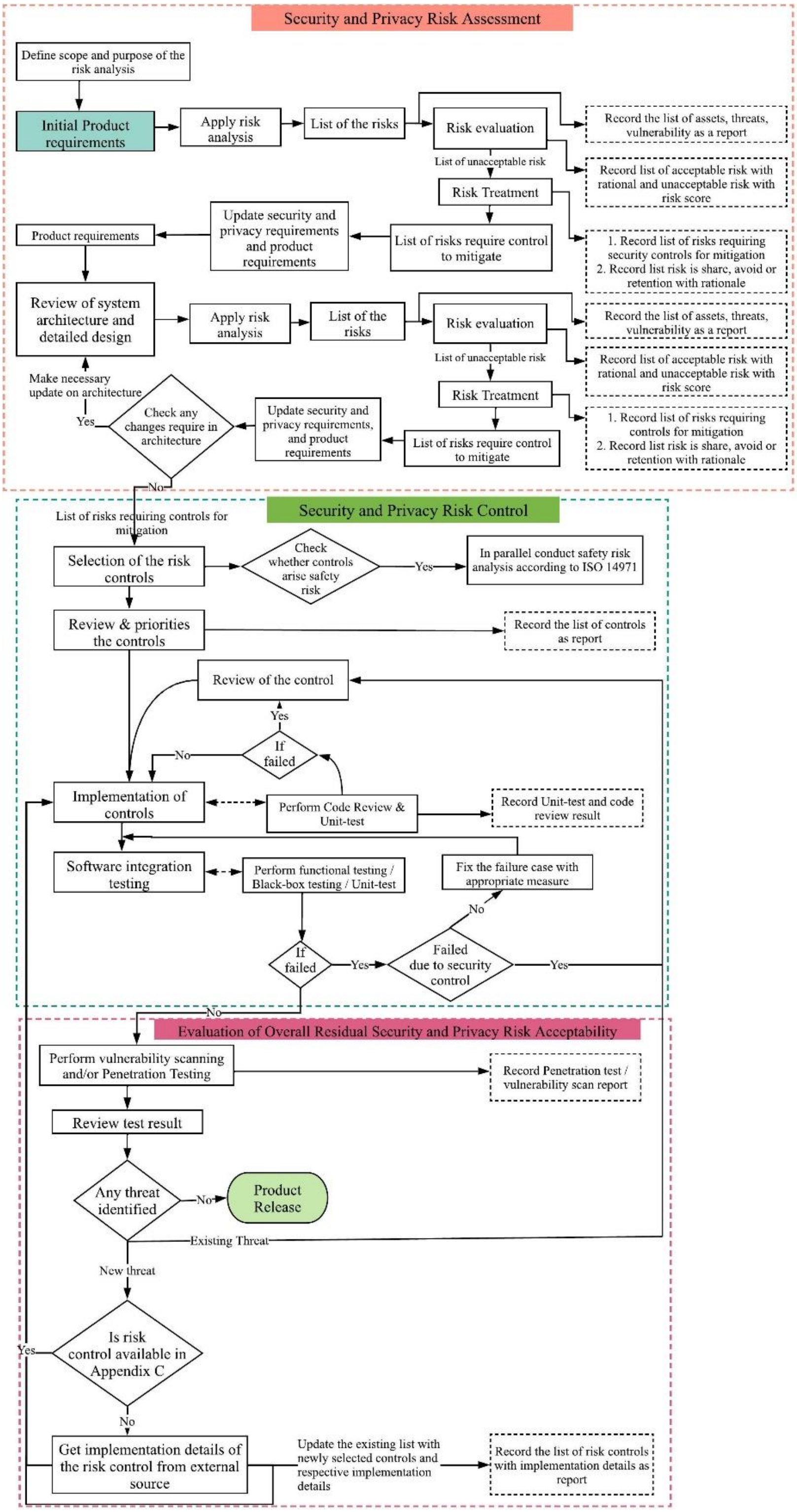

Security and Privacy Risk Assessment
Define scope and purpose of the risk analysis
Initial Product requirements
Apply risk analysis
List of the risks
Risk evaluation
Record the list of assets, threats, vulnerability as a report
List of unacceptable risk
Record list of acceptable risk with rational and unacceptable risk with risk score
Risk Treatment
Product requirements
Update security and privacy requirements and product requirements
List of risks require control to mitigate
1. Record list of risks requiring security controls for mitigation
2. Record list risk is share, avoid or retention with rationale
Review of system architecture and detailed design
Apply risk analysis
List of the risks
Risk evaluation
Record the list of assets, threats, vulnerability as a report
List of unacceptable risk
Record list of acceptable risk with rational and unacceptable risk with risk score
Make necessary update on architecture
Yes
Check any changes require in architecture
Update security and privacy requirements, and product requirements
Risk Treatment
List of risks require control to mitigate
1. Record list of risks requiring controls for mitigation
2. Record list risk is share, avoid or retention with rationale
No
Security and Privacy Risk Control
List of risks requiring controls for mitigation
Selection of the risk controls
Check whether controls arise safety risk
Yes
In parallel conduct safety risk analysis according to ISO 14971
Review & priorities the controls
Record the list of controls as report
Review of the control
Yes
If failed
No
Implementation of controls
Perform Code Review & Unit-test
Record Unit-test and code review result
Software integration testing
Perform functional testing / Black-box testing / Unit-test
Fix the failure case with appropriate measure
No
If failed
Yes
Failed due to security control
Yes
No
Evaluation of Overall Residual Security and Privacy Risk Acceptability
Perform vulnerability scanning and/or Penetration Testing
Record Penetration test / vulnerability scan report
Review test result
Any threat identified
No
Product Release
Existing Threat
New threat
Is risk control available in Appendix C
Yes
No
Get implementation details of the risk control from external source
Update the existing list with newly selected controls and respective implementation details
Record the list of risk controls with implementation details as report

Figure Appendix B- 1: Data security and privacy framework for WBAN application

1) Risk analysis
2) Risk evaluation
3) Risk control selection and implementation
4) Evaluation of overall risk acceptability
5) Risk management reporting
6) Post-production information

The proposed framework takes product requirements as an input to identify the risks using the risk analysis process. However, this framework does not perform any validation or verification of the quality of the product requirements. To develop quality product requirements, guidelines provided by ISO/IEC 62304 can be utilised. One of the key stages of this framework is to identify the security and privacy controls to mitigate the risk. The controls are identified by considering the potential security and privacy weaknesses of WBAN application ecosystems and mapping security and privacy weaknesses against controls in available standards. The aforementioned standards and guidelines include:

1) ISO/IEC 80001-2-2 (Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls): IEC/TR 80001-2-2 is a technical report that provides background processes to address security and risk related capabilities for connecting medical devices to IT-networks (IEC 80001-2-2, 2011). The IEC/TR 80001-2-2 technical report also presents a total of nineteen high-level security capabilities to maintain the confidentiality, integrity and availability of data.
2) ISO/IEC 80001-2-8 (Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2): IEC/TR 80001-2-8

is a technical report which provides guidance to Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) to establish security controls for applications with security capabilities which are outlined in IEC/TR 80001-2-2 (ISO/IEC 80001-2-8, 2016). The IEC/TR 80001-2-8 technical report was developed to establish security controls for the 19 security capabilities mentioned in the IEC/TR 80001-2-2. These controls come from six different international standards.

3) NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) - The NIST 800-53 standard provides security and privacy controls to protect the application, data, assets and organisations from a diverse set of attacks, threats and risks (NIST SP800-53, 2020). These controls support the development of secure and resilient federal information systems that meet the requirements set by the Federal Information Security Management Act (FISMA). This guideline applies to any component of a system which stores, processes and transmits information. NIST SP 800-53 provides controls for the operational level, the technical level and the management level of information systems. These controls are used to assure confidentiality, integrity and availability of the federal information system.

4) ISO/IEC 27002 (Information technology — Security techniques — Code of practice for information security controls): ISO 27002 is an information security standard developed by International Organization for Standardization (ISO) which provides best practice recommendations and information security controls to assure confidentiality, integrity, and availability of data (ISO/IEC 27002, 2017). This standard is designed for organisations to use as a reference to guide organisations to select, implement, and manage controls based on ISO/IEC 27001 to minimise security and privacy risk. Additionally, this standard also helps for developing industry and organisation-specific

information security management guidelines by considering their specific information security and privacy risk environment.

5) ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines)
6) ISO/IEC 27799 (Health informatics — Information security management in health using ISO/IEC 27002) (ISO 27799, 2016)

The standards and guidelines were used to identify the relevant controls and their implementation details. However, these standards provide very high-level implementation details for controls, so other external sources such as NIST 800-175B (Barker, 2016), NIST 800-56A (Barker, Chen and Moody, 2014), RFC 6749 (6749, no date), OWASP, blogs and research papers were used to further develop security and privacy control implementation details. A detailed description of the security and privacy control selection process for WBAN applications is outlined in section 5.1 under Chapter 4. Additionally, the implementation detail for each security and privacy control is presented in Appendix C.

The final stage of the framework is to evaluate the effectiveness of each security and privacy control with regards to mitigating the identified threats. As recommended by IEC/CD 80001-5-1(IEC 80001-5-1, 2020) and TIR 57, this framework has adopted the use of code review, unit testing, software integration testing, vulnerability scanning and penetration testing to evaluate the effectiveness of the security and privacy controls. Finally, the result of each stage is documented in a risk management report. This framework's implementation process is presented in section 4 under Appendix B.

Additionally, an organisation needs to define a team to carry out this framework's implementation process. Table Appendix B- 1 outlines the respective task of each role related to the implementation of the framework. In the case of limited resource in the organisation, a single resource can carry out multiple roles and conduct more than one task.

Table Appendix B- 1: Team structure for implementing the proposed framework

Task No	Task Definition	Key Roles
1	Defining the scope	*Executives, ** Management, *** Assessor
2	Risk analysis	Management, Assessor, ****Third-party resource (if needed)
4	Risk evaluation	Executives, Management, Assessor
5	Risk control	Management, Assessor, Third-party resource (if needed)
7	Evaluation of overall residual risk acceptability	Assessor, Management, Third-party resource (if needed)

** Executives: C-level executives of the organisations*
*** Management: Product manager, Project manager, Team Lead, QA Lead*
**** Assessor: Technical Lead, Software Architect, Product Owner, Senior Software Engineer, Senior QA Engineer*
**** *Third-party resource:* Consultant, Penetration tester

4 Implementation Process

This section provides the guidelines for implementing the process detailed in Figure Appendix B- 1. The implementation process consists of three key stages which are described below:

1) Security and privacy risk assessment
2) Security and privacy risk control
3) Evaluation of overall residual security and privacy risk acceptability

4.1 Security and Privacy Risk Assessment

The security and privacy risk assessment helps to identify, analyse and evaluate potential security and privacy risks. This assessment will help an organisation to make decisions about which risks require security and privacy controls for mitigation, and which risks are acceptable. Risk assessment should be performed as early as possible to avoid fundamental flaws in the application design whose removal in later lifecycle phases is very costly. As a result, risk assessment needs to be repeatedly applied in the different phases of lifecycle; starting with the security and privacy requirements, system architecture, then implementation, deployment, operation. This framework will take initial product requirements as an input to conduct the security and privacy risk assessment in the requirement analysis phase. Figure Appendix B- 2 illustrates the steps to conduct the security and privacy risk assessment in requirements analysis and system architecture phase.

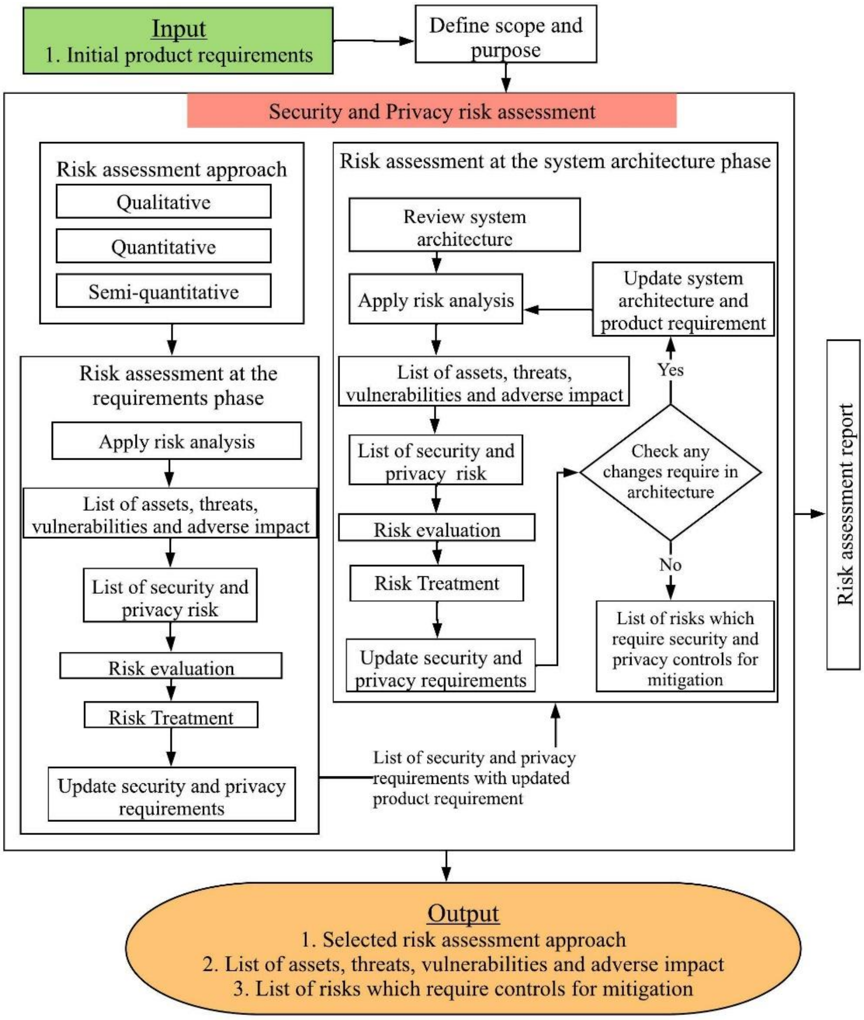

Input
1. Initial product requirements
Define scope and purpose
Security and Privacy risk assessment
Risk assessment approach
Qualitative
Quantitative
Semi-quantitative
Risk assessment at the requirements phase
Apply risk analysis
List of assets, threats, vulnerabilities and adverse impact
List of security and privacy risk
Risk evaluation
Risk Treatment
Update security and privacy requirements
List of security and privacy requirements with updated product requirement
Risk assessment at the system architecture phase
Review system architecture
Apply risk analysis
Update system architecture and product requirement
List of assets, threats, vulnerabilities and adverse impact
Yes
List of security and privacy risk
Check any changes require in architecture
Risk evaluation
No
Risk Treatment
List of risks which require security and privacy controls for mitigation
Update security and privacy requirements
Risk assessment report
Output
1. Selected risk assessment approach
2. List of assets, threats, vulnerabilities and adverse impact
3. List of risks which require controls for mitigation

Figure Appendix B- 2: Steps to conduct a security and privacy risk assessment

The security and privacy risk assessment is divided into two key stages:

- Risk analysis
- Risk evaluation and treatment

The Risk analysis stage aims to identify the assets, threats, vulnerabilities and adverse impacts on an application. To assist with the risk analysis, an organisation may use relevant information obtained from a previously risk analysis of a similar type of product as a starting point. The degree of reusability of data from previous analyses depends on the difference between the applications from a security perspective. The risk evaluation and treatment stage will help to identify the acceptable risks and unacceptable risks which will require security and privacy controls.

The rest of the section is organised as follows; section 4.1.1 provides guidance on defining the scope and purpose of the risk analysis. Following this, section 4.1.2 presents three risk assessment approaches with advantages and disadvantages. Section 4.1.3 details the steps to conduct the risk analysis and risk evaluation with risk treatment during the requirements analysis phase. Section 4.1.4 details the lists of design principles which need to be taken into consideration while developing the system architecture and conducting the risk analysis and risk evaluation with risk treatment during the system architecture phase. Finally, section 4.1.5 provides the list of items which will be included in the security and privacy risk assessment report.

4.1.1 Define scope and purpose

Before conducting the security and privacy risk assessment, organisations need to define and document the purpose and scope of the assessment. The scope will include:

- The intended use
- Initial product requirements
- Operating environment of the application
- List of team members presented in Table Appendix B- 1 who will conduct the risk analysis and risk evaluation.
- Timeline for the security and privacy risk assessment should be provided.

4.1.2 Risk assessment approach

There are three different risk assessment approaches - qualitative, quantitative and semi-quantitative (AAMI TIR57, 2016). Each of these approaches provides a standard approach to help an organisation and decision-makers to assess the consequences of threats and vulnerabilities. The rest of the section will present details about each approach and a comparison of the three approaches.

Qualitative: A qualitative assessment approach uses a scale of qualifying attributes (e.g. Very Low, Low, Medium, High, Very High) to describe the impact and likelihood of potential consequences of threats and vulnerabilities. A qualitative assessment approach uses subjective values for the impact and likelihood of threats and vulnerabilities. Below is the definition for different scales from Appendix I of NIST 800-30 (NIST:800-30, 2012) :

- Very High: Almost certain that threat event will occur, and vulnerabilities will be exploited. If the threat event occurs then it will cause multiple catastrophic adverse effects on application operations, business goal, loss of assets
- High: Highly likely that threat event will occur, and vulnerabilities will be exploited. If the threat event occurs then it will cause catastrophic adverse effects on application operations, business goal, loss of assets
- Medium: Somewhat likely that threat event will occur, and vulnerabilities will be exploited. If the threat event occurs then it will cause serious adverse effects on application operations, business goal, loss of assets
- Low: Unlikely that the threat event will occur or exploit vulnerabilities. If the threat event occurs, it will have limited adverse effects on application operations, business goal, loss of assets

- Very Low: Highly unlikely that threat event will occur, and vulnerabilities will be exploited. If the threat event occurs then it will have negligible adverse effects on application operations, business goal, loss of assets

The value of the impact and likelihood depends on the experience, expertise and competence of the person conducting the risk assessment. As qualitative values are estimated subjectively, to achieve repeatability of the assessment process, it is necessary to assure that process is unambiguous. The qualitative assessment approach is very easy and less time consuming to perform compared to quantitative and semi-qualitative approaches, as this approach does not require any special tools or methods to conduct the risk assessment.

Quantitative: Quantitative risk assessments use a scale with numerical values based on a set of mathematical methods, rules and historical incident data. This approach is usually expressed in a monetary term which reflects the amount of money an organisation may lose over a time period if the threat event occurs or a vulnerability is exploited. There are several mathematical formulas available to calculate the annual loss expectancy, single loss expectancy, and safeguard cost if the threat event occurs or a vulnerability is exploited. The annual loss expectancy can be calculated by using $Risk\ R = Assets\ Value * Exposure\ factor * Probability\ of\ threats\ and\ vulnerabilities$. For example, the risk of malware attack on web server which asset value is \$10000, the exposure factor due to the attack is 40% and probability of attack occurrence in a year is 20% then the annual loss will be $R = \$10000 * 0.4 * 0.2 = \$800/year$. The quality of the analysis depends on the accuracy of the numerical values, historical incident data and the validity of the methods used. By using the same mathematical model and historical incident data, the organisation can easily reproduce and replicate the same numerical value.

Semi-quantitative: A semi-quantitative risk assessment provides an intermediate level between the qualitative and quantitative risk assessment. To evaluate a security and privacy risk using a semi-quantitative approach, use bins (e.g. 0-4, 5-20, 21-79, 80-95, 96-100) and scales (e.g. 1-10) which will provide the textual evaluation of qualitative risk assessment and the numerical evaluation of quantitative risk assessment. The value of the bins and scales will help to communicate the risk to decision-maker as well as to perform a relative comparison of risk. This approach does not require the same level of skill, tools, mathematical methods and historical incident data as in quantitative risk assessment. Semi-quantitative risk assessment is most useful in providing a structured way to rank risks according to their likelihood and impact. All three approaches have advantages and disadvantages. Quantitative risk assessment requires historical data to determine the likelihood of a threat event occurring or a vulnerability being exploited. Historical data that is not recently updated may add additional error to the risk assessment. For example, historical data for the likelihood of a threat event occurring due to using a particular algorithm might be high. If the data is not recent, then it may mislead the evaluation of that particular threat. Furthermore, it is difficult to calculate the cost of organisation reputational damage, loss of competitive advantage and harm to user health if any threat event occur or a vulnerability being exploited. Due to these facts, the quantitative approach will not be appropriate in information security and privacy risk assessment. This framework will use qualitative and semi-quantitative assessment approaches for evaluating the security and privacy risk. Table Appendix B- 2 outlines the key advantages and disadvantages of each approach. This comparison of the approaches will also help the security and privacy risk evaluation team to choose the appropriate approach to evaluate each risk. How to determine the impact and likelihood of risks using qualitative and semi-quantitative approaches is presented in section 4.1.3.2.

Table Appendix B- 2:Advantages and disadvantages for Qualitative, Quantitative and Semi-quantitative approaches

	Advantage	Disadvantage
Qualitative	• Quick and easy to perform • Subjective evaluation of probability and impact • Ease of understanding by all relevant personnel • No special software or tools required	• Subjective • Dependence on the subjective choice of the scale • Short-range of values make it difficult for risk comparison and prioritisation • Different experts with individual experience may produce different assessment results • The result depends on the quality of the risk management team
Quantitative	• Provides precise information that company leaders can use to determine the impact of risks • Risk are sorted by their financial impact and assets by their financial value • Probabilistic estimates of time and cost • Repeatability, and reproducibility of assessment results	• The method of calculation is complex • Time-consuming • May require specialised tools or methods • Lack of historical data on new risks or information security weaknesses will create an illusion of worth and accuracy of the risk assessment
Semi-quantitative	• Provides a more consistent and rigorous approach compare to qualitative approach for assessing and comparing risks • Risk assessment covers a wider range of probability and impact • Does not require specialised tools or methods like quantitative assessment approach	• Time-consuming

4.1.3 Risk assessment at the requirements phase

The objective of conducting a risk assessment at the requirement analysis phase is to identify the security and privacy risks, evaluate the identified risks, apply risk treatment to identify the risks which will require controls to mitigate and develop the security and privacy requirements. The initial product requirements and risk assessment approach will be taken as an input to conduct the risk assessment at this phase. Figure Appendix B- 3 illustrates the steps to conduct a risk assessment at the requirements analysis phase.

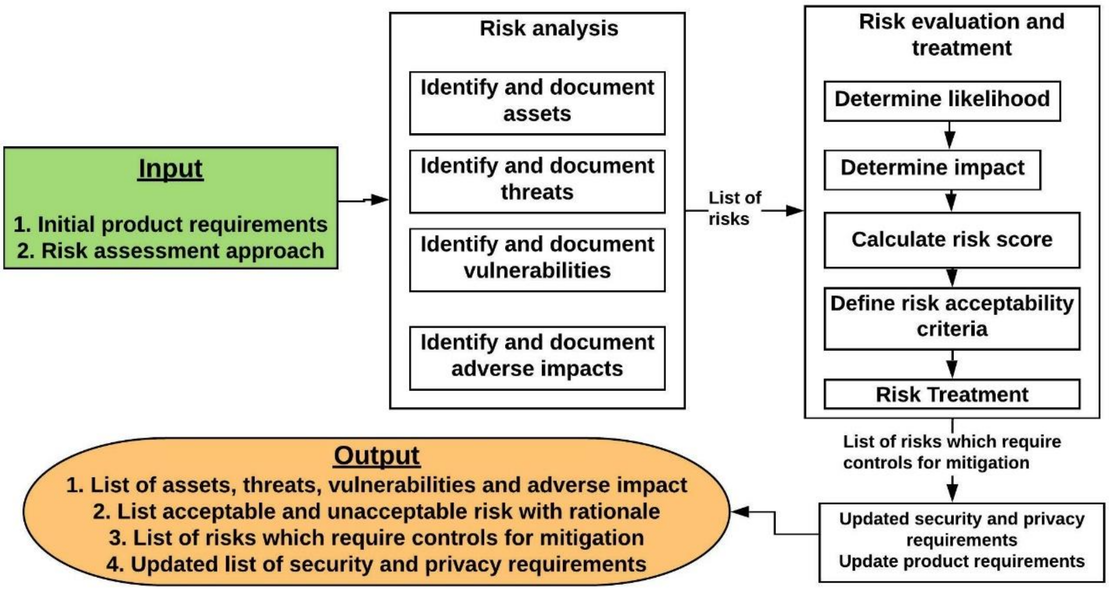

Input
1. Initial product requirements
2. Risk assessment approach
Risk analysis
Identify and document assets
Identify and document threats
Identify and document vulnerabilities
Identify and document adverse impacts
List of risks
Risk evaluation and treatment
Determine likelihood
Determine impact
Calculate risk score
Define risk acceptability criteria
Risk Treatment
List of risks which require controls for mitigation
Updated security and privacy requirements
Update product requirements
Output
1. List of assets, threats, vulnerabilities and adverse impact
2. List acceptable and unacceptable risk with rationale
3. List of risks which require controls for mitigation
4. Updated list of security and privacy requirements

Figure Appendix B- 3: Risk assessment steps in the requirement analysis phase

Below is the list of key tasks to be conducted during the risk assessment at the requirements analysis phase:

- Apply risk analysis to identify the security and privacy risk
- Evaluate each security and privacy risk to identify the acceptable and unacceptable risk
- Update list of security and privacy requirements for unacceptable risk

The rest of the section is organised as follows; section 4.1.3.1 provides guidance on identifying security and privacy risks by conducting risk analysis while section 4.1.3.2 details steps to evaluate the security and privacy risks and identify the list of unacceptable risks which will require security and privacy controls to mitigate. Finally, section 4.1.3.3 outlines the list of updated security and privacy requirements that need to be taken into consideration.

4.1.3.1 Security and privacy risk analysis

As part of the security and privacy risk analysis, the following four tasks need to be conducted. Of the following four tasks, identify and document threats and identify and document vulnerabilities can be performed in any order.

1) **Identify and document the assets:** An asset is valuable and needs to be protected to keep the application operating safely and securely. Assets associated with IT systems usually fall into one of three classes: a) information, b) processes and c) physical. Information assets represent data that is of value to the owning organisation. Examples of types of information assets are: general data, system data, specialist databases and client data. Process assets represent applications, where data is transformed or analysed. The distinction from information assets is that the associated data is of little value without the processing capabilities of the related applications. Examples of types of process assets are: financial, communication, logistical, manufacturing and office automation. Physical assets represent the actual information processing equipment used to support the information and process assets. Examples of types of physical assets are: critical network infrastructure, portable PCs and data centers. Assets of a WBAN application include sensor devices, information collected by the sensor devices, and server instances which are used to process and store the data. If the application interfaces with any external services such as third-party libraries or third-party application services, these also need to be taken into consideration during the asset identification process. The assets will be documented in the security and privacy risk assessment report, along with the date that the assets were identified, and the name of the persons with their role as presented in Table Appendix B- 1 under section 3. Figure Appendix B- 4 illustrates the list of assets for general WBAN applications which can be used as a starting point for the asset identification process:

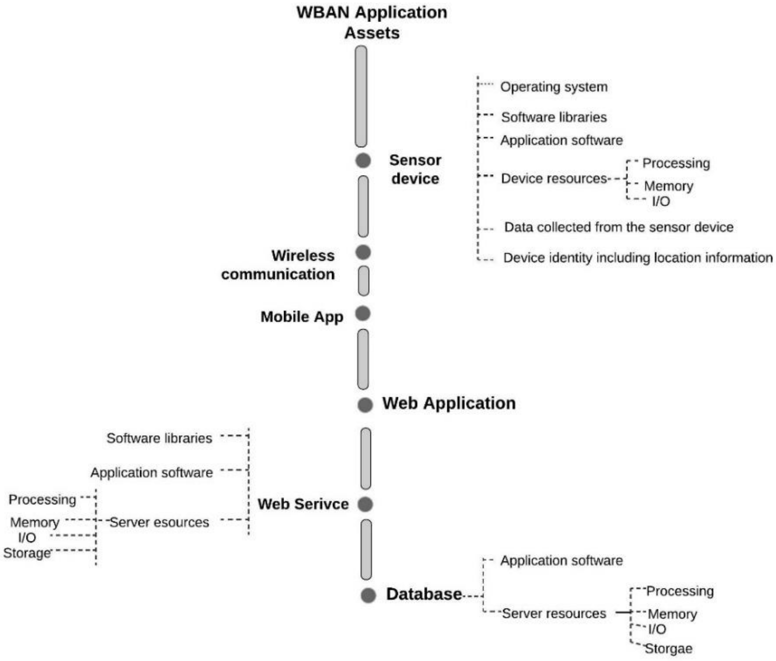


Figure Appendix B- 4: List of assets for WBAN applications

2) **Identify and document threats:** A threat is any circumstance or event with the potential to impact application assets by exploiting a vulnerability adversely. A threat event originates from a threat source. NIST 800-30 defines a threat source as *"the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability"* (NIST:800-30, 2012). Threat sources can be adversarial or non-adversarial. Adversarial threats are initiated by individuals, groups, organisations, or nation-states who have the technical capability to attack an application to gain access to the information, the network or other computing equipment. The group of people who carry out adversarial threats are known as threat agents/actors. A threat agent can be inside the organisation, or external such as cybercriminals and hacktivists. During the risk analysis, the following considerations needs to taken into account: the threat actor's skill level; the threat actor's motivation; and the potential gain from an exploit. Additionally, an organisation also needs to

consider non-adversarial threats, such as a natural event, to support high availability, technical failure of any component, software and capacity saturation.

To identify threats to a WBAN application, the assessor team comprised of the technical lead, software architect, product owner, and senior software engineer needs to perform the following three steps:

a) Using Table Appendix E-1 in Appendix E, select the threats related to the assets you have identified.

b) As the threat landscape is changing rapidly, it is recommended to check for newly discovered threats at the time when the threat identification process is being conducted. To gather information about newly discovered threats, the assessor team can use various sources such as research articles, blog posts, open-source platforms such as OWASP[1], governmental agencies such as US-CERT[2], European Union Agency for Cybersecurity (ENISA)[3], NIST[4], Federal Office for Information Security (BSI)[5], STRIDE, Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), U.S. National Vulnerability Database (NVD), BSI Top 10 threats, and Mitre ATT&CK for ICS and private organisations such as HITRUST[6]. Additionally, threats related to technology stack use for developing the application also need to take in consideration. Each newly discovered threat needs to be analysed by studying the threat description, threat agents, possible attack scenarios and checking whether the same attack scenario can occur within

[1] https://owasp.org/www-community/attacks/

[2] https://www.us-cert.gov/resources/cybersecurity-framework

[3] https://etl.enisa.europa.eu/

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[5] Federal Office for Information Security (BSI)

[6] https://hitrustalliance.net/threat-catalogue/

the WBAN application. If a newly discovered threat is a legitimate threat for WBAN applications, then the assessor team needs to identify the assets which will be affected if the threat occurs.

c) Document below the list of items in the security and privacy risk assessment report:

   - List of threats and respective affected assets
   - Date when the threat identification was conducted,
   - The name and role of the person who conducted the threat identification

3) **Identify and document the vulnerabilities:** A vulnerability is a weakness of an application which could be exploited by a threat source or threat events. Vulnerabilities can be introduced due to conscious design decisions to include or bypass a control, errors in the design, errors during the implementation, or wrong configuration of the device by the end-user. Vulnerabilities need to be identified at both the requirements and the design architecture phases. To identify vulnerabilities, the assessor team comprising of the technical lead, software architect, product owner, and senior software engineer need to perform the following steps:

   a) Review the list of vulnerabilities presented in Appendix E and select which are related to the assets identified during the asset identification process.

   b) As the vulnerability landscape is constantly changing, the team also need to check for new vulnerabilities in various sources such as OWASP IoT Top 10[7] and OWASP Mobile Top 10[8]. Additionally, vulnerabilities related to technology stack use for developing the application also need to take in

[7] https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[8] https://owasp.org/www-project-mobile-top-10/

consideration. During the review of a newly discovered vulnerability, the team needs to review the common security weaknesses and possible threat scenario section, in order to check whether the vulnerability can be exploited by any threat and affect any assets identified during the asset identification process.

c) Finally, the assessor team will document all the vulnerabilities in a security and privacy risk assessment report. This report will include the vulnerability name, affected assets, name and role of the person who conducted the vulnerability identification process and the date when the vulnerability identification process was conducted.

4) **Identify and document the adverse impacts:** An adverse impact of a security breach can be described in terms of loss or degradation of confidentiality, integrity, availability and privacy of data. TIR 57 outlines a set of questions to identify the adverse impact of compromised assets. This framework has extended those questions by the addition of point d) below:

a) What is the impact if that asset's confidentiality is compromised, and the information it contained is make available to an attacker?

b) What is the impact if that asset's integrity is compromised?

c) What is the impact if that asset is made unavailable?

d) What is the impact if that asset's privacy is compromised?

e) Can the immediate impact of a compromised asset lead to another type of attack or vulnerability?

The members of the assessor team will review each threat and vulnerability and ask the above questions to identify the adverse impacts. For example, if the attacker launches a DoS attack on the webserver and makes the service unavailable, it will have an impact on the service operation and business mission. Finally, the team will document the adverse impact of each threat and vulnerability in the security and privacy risk assessment report.

4.1.3.2 Risk Evaluation and treatment

The risk evaluation process helps an organisation to determine whether the identified threats and vulnerabilities are acceptable or not by calculating the impact and likelihood level. As the calculation of the impact and likelihood of the risk will be subjective, organisations can employ additional resource or onboard external expert to conduct the calculation. Onboarding additional resource will help to mitigate the bias and assure the reproducibility of calculation. Alternatively, orgnisation can use binary approach “possible” or “impossible” to evaluate the risk. During risk evaluation using a binary approach organisation can use information obtained from the below sources:

- published standards
- security and privacy investigation reports
- data from similar applications already in use, including publicly available reports of incidents
- expert opinion

Furthermore, risk treatment will help an organisation to decide how each unacceptable risk will be addressed. The organisation should include the team members presented in Table Appendix B- 1 comprised of the technical lead, product owner, project manager, and senior software engineer to perform the security and privacy risk evaluation and risk treatment. Figure Appendix B- 5 illustrates the steps to conduct security and privacy risk evaluation and risk treatment.

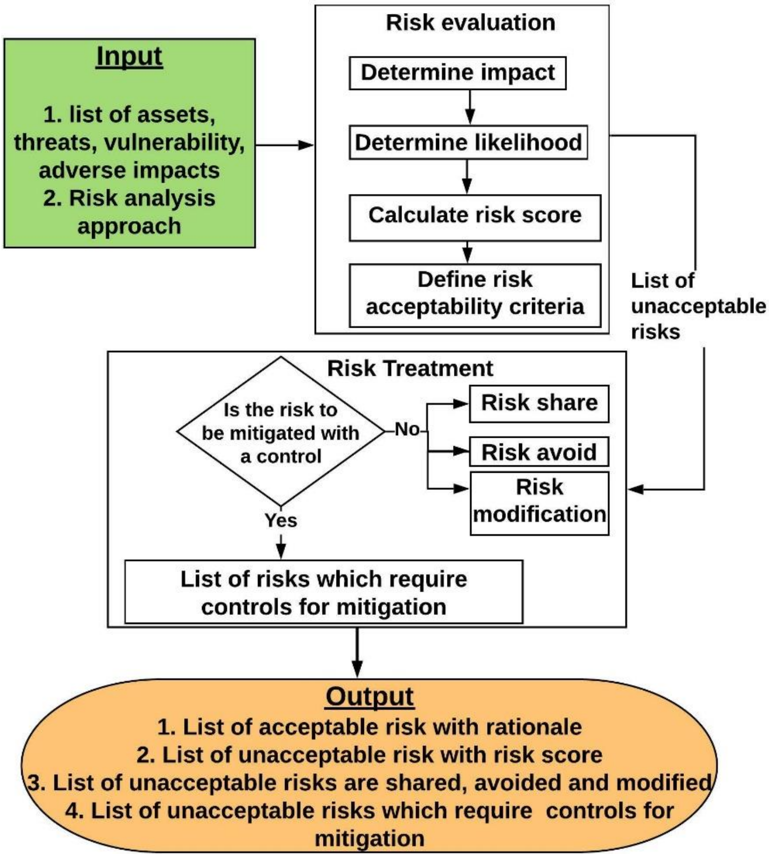

Input
1. list of assets, threats, vulnerability, adverse impacts
2. Risk analysis approach
Risk evaluation
Determine impact
Determine likelihood
Calculate risk score
Define risk acceptability criteria
List of unacceptable risks
Risk Treatment
Is the risk to be mitigated with a control
No
Yes
Risk share
Risk avoid
Risk modification
List of risks which require controls for mitigation
Output
1. List of acceptable risk with rationale
2. List of unacceptable risk with risk score
3. List of unacceptable risks are shared, avoided and modified
4. List of unacceptable risks which require controls for mitigation

Figure Appendix B- 5: Steps to conduct a risk evaluation and risk treatment

1) Determine Impact

Impact refers to the extent to which a threat event might affect the application. Impact assessment criteria may include:

- Loss of assets
- Operational impacts
- Harm to user health
- Reputational harm
- Financial loss

The assessor team also needs to consider the asset's valuation while calculating the impact score of a threat. An asset's valuation will include the criticality of the threat on the asset, the importance of that asset to fulfil the business objectives, the replacement value of the asset and the business consequence due to the asset being lost or compromised. For example, a physical attack on a sensor device or a database will have different impacts on business operations. A physical attack on a sensor will only compromise that particular sensor device. If the database is compromised and data is lost, then it will have a much larger impact on financial, reputation, regulatory consequences and the operation of the application. Table Appendix B- 3 outlines the assessment scale for calculating impact scores. Finally, the impact score for each threat and vulnerability needs to be documented in the security and privacy risk assessment report.

Table Appendix B- 3: Assessment scale for Impact

Qualitative Values	**Semi-quantitative Values**		**Impact to Objectives**
	scale	bins	
Very Low (1)	0-4	0	Threat event will have negligible adverse effects on application operations, business goal, loss of assets
Low (2)	5-20	2	Threat event will have limited adverse effects on application operations, business goal, loss of assets
Medium (3)	21-79	5	Threat event will have serious adverse effects on application operations, business goal, loss of assets
High (4)	80-95	8	Threat event will have catastrophic adverse effects on application operations, business goal, loss of assets
Very High (5)	96-100	10	Threat event will have multiple catastrophic effects on application operations, business goal, loss of assets

Table Appendix B- 4 illustrated an example for identifying the impact level of physical attack on a sensor node. During the calculation, the impact level value is assigned to each impact factor. Finally, the overall impact level score is calculated by taking the average of all the factors value. So, the overall impact level for a physical attack on the sensor device is calculated as *"Medium"*.

Table Appendix B- 4: Impact analysis for physical attack on a sensor node

Impact factor	**Impact description**	**Impact Level**		
		Qualitative	**Semi-quantitative**	
			scale	**bins**
Loss of assets	Only the sensor device will be lost	Medium	30	5
Operational impacts	Only the sensor device will be out of operation, it will not severely affect the overall application operation	Medium	30	5
Harm to user health	Only the person who is using the device will be in risk	Very High	100	10
Reputational harm	Loss of a single sensor device will not create severe reputational harm	Medium	40	5
Financial loss	Loss of a single device will have limited financial impact	Low	10	2
Average		**Medium**	**70**	**5.2**

2) Determine Likelihood

The likelihood represents the probability that a threat event will occur by exploiting one or more vulnerabilities. To estimate the likelihood, the assessor team needs to consider factors such as:

- Adversary intent
- Adversary skill level
- The affected asset
- Historical evidence about the threat

The same threat can have a different likelihood score based on the source of the threat and assets affected. For example, a DoS attack is a widely known attack in WBAN applications which compromises the availability of the web server and sensor devices. Initiating a DoS attack on a web server will be easier than launching the same attack on the sensor device as a sensor device attack will require the adversary to have advanced level skills and tools. In this scenario, the likelihood level of an attack on the web server will be different to that of an attack on the sensor. So, during the assessment the assessor team needs to assign the likelihood level based on the available evidence, experience and expert judgement. Table Appendix B- 5: outlines the assessment scale for calculating likelihood level. Finally, the likelihood level for each threat and vulnerability needs to be documented in the security and privacy risk assessment report.

Table Appendix B- 5: Assessment scale for Likelihood

Qualitative Values	**Semi-quantitative Values**		**Likelihood score definition**
	scale	bins	
Very Low (1)	0-4	0	Highly unlikely to threat event occurs or exploit the vulnerabilities
Low (2)	5-20	2	Unlikely to threat event occurs or exploit the vulnerabilities
Medium (3)	21-79	5	Somewhat likely to threat event occurs or exploit the vulnerabilities
High (4)	80-95	8	Highly likely to threat event occurs or exploit the vulnerabilities
Very High (5)	96-100	10	Almost certain to threat event occurs or exploit the vulnerabilities

Table Appendix B- 6 illustrated an example for identifying the likelihood level for DoS attack on a web server. During the calculation, the likelihood level value is assigned to each likelihood factor. Finally, the overall likelihood level score is calculated by taking the average of all the factors value. So, the overall likelihood level for likelihood is calculated as *"Very High"*.

Table Appendix B- 6 : Likelihood analysis for DoS attack on a web server

Likelihood factor	Likelihood description	Likelihood Level		
		Qualitative	Semi-quantitative	
			scale	bins
Adversary intent	Make the whole application unavailable	Very High	100	10
Adversary skill level	Requires medium level skill to launch the attack	High	90	8
Affected asset	All assets that depend on the web server including the web server itself	Very High	100	10
Historical evidence	Very common and well-known attack for web server	Very High	100	10
Average		**Very High**	**97.5**	**9.5**

3) Calculate risk score

The aim of this stage is to calculate the risk score based on the impact and likelihood of threats and vulnerabilities. Appendix I of NIST 800-30 details how to calculate the risk score by multiplying impact times likelihood (NIST:800-30, 2012). Alternatively, the team can use the CVSS risk score calculator to calculate the risk score (NIST, 2020). A sample risk score matrix using a qualitative assessment approach and the risk score calculation from NIST 800-30 is presented in Table Appendix B- 7 . Finally, the risk score needs to be documented in the security and privacy risk assessment report.

Table Appendix B- 7 : Rrisk score matrix for qualitative approach

		Likelihood				
		Very Low (1)	**Low (2)**	**Medium (3)**	**High (4)**	**Very High (5)**
Impact	**Very High (5)**	**5**	**10**	**15**	**20**	**25**
	High (4)	**4**	**8**	**12**	**16**	**20**
	Medium (3)	**3**	**6**	**9**	**12**	**15**
	Low (2)	**2**	**2**	**6**	**8**	**10**
	Very Low (1)	**1**	**2**	**3**	**4**	**5**

4) Risk acceptability criteria

Risk acceptability criteria will help the organisation to identify whether the threats and vulnerabilities are acceptable or unacceptable based on a set of criteria defined by the security evaluation team. There are no standard guidelines available to define the set of criteria. However, the team can consider various factors while defining the criteria such as;

- The organisation’s goals and objectives
- Business operations
- Application use case and operation
- The technology stack used for developing the application
- Legal and regulatory aspects
- Budget and time frame for developing the application

Table Appendix B- 8 outlines the security and privacy risk acceptability criteria based on the risk score calculated using the qualitative approach. The proposed criteria treat the risks with a low or very low score as acceptable risks, and risks with medium, high and very high as unacceptable risks. If required, the evaluation team can also make a judgment on the selection criteria. For example, a natural disaster on the database server can have very high impact with medium likelihood which makes.

Table Appendix B- 8: Risk acceptability criteria (Qualitative approach)

Risk Score	**Semi-quantitative Values**		**Description**
	scale	bins	
Very Low	0-4	0	The risks are acceptable. Plans to reduce and mitigate the risk should be included in future plans and budgets.
Low	5-20	2	The risk may be acceptable over the short term. Plans to reduce and mitigate risk should be included in future plans and budgets.
Medium	21-79	5	The risk is unacceptable. Measures to reduce and mitigate the risk should be implemented as soon as possible.
High	80-95	8	The risk is unacceptable. Immediate measures to reduce and mitigate the risk should be implemented as soon as possible.
Very High	96-100	10	The risk is totally unacceptable. Immediate measures must be taken to mitigate the risk.

To mitigate this threat, an organisation might need an additional database server as a backup which will incur additional costs and resources. In this scenario, the team might decide to treat this risk as acceptable for a certain period. If the team makes this type of adjustment on the risk acceptability criteria, then each affected risk needs to be documented along with the rationale in the security and privacy risk assessment report. Finally, all unacceptable and acceptable risks with the rationale need to be documented in the security and privacy risk assessment report.

5) Risk Treatment

Upon identifying the unacceptable risks of the application, the next task is to identify what measures will be required to address these risks. Risk Treatment is the process of selecting and implementing measures to address the risk. There are three options available for risk treatment measures which include:

- Risk modification: A risk which requires implementation of safeguards or controls to reduce the impact and/or likelihood to an acceptable level.
- Risk avoidance: A risk can be avoided by eliminating the source of the risk or the asset exposed to the risk. This is usually applied when the severity of the risk impact and/or likelihood outweighs the benefits gained from implementing the countermeasure. For example; physically moving an on-premises information processing facility to an alternative location to mitigate the risk caused by nature might be outweighed with the cost of moving the facilities.
- Risk sharing: A risk can be fully or partially shared or transferred to another party. If the application is using any third-party libraries, third-party devices or public cloud services, risk related to these can be shared or transferred to the owner of the service. For example, while developing a cloud-based application, risk related to disk

encryption of the database can be transferred to the cloud service provider to mitigate the risk.

The security and privacy risk evaluation team will evaluate each unacceptable risk taking the above possible risk treatment options into account. This will result in a list of security and privacy risks which security and privacy risk controls. Finally, the team will also record the list of risks that require security and privacy risk controls, shared risks and avoided risks with rational in the risk assessment report.

4.1.3.3 Update security and privacy requirements

The goal of this stage is to update the security and privacy requirements with the lists of security and privacy risks, identified in the previous stage, which require security and privacy controls to mitigate. The list of security and privacy risk controls outlined in Appendix B can be taken in consideration. As risk analysis on the requirement analysis stage uses the initial product requirements, the updated security and privacy requirements will feed into the final product requirements for the application. The following security and privacy requirements can be used as a starting point:

- Assure data confidentiality by protecting sensor nodes and/or database server from unauthorised access and leaking while data is at-rest. Use access control and an authentication process to protect from unauthorised access
- Assure data integrity by protecting data from external modification during transmission or while in storage. Use data encryption and checksum check to assure data integrity
- Implement proper authentication and authorisation process to check the identity of the user before allowing access to the data
- Assure that data will be always available to an authorised entity of the application

- Assure privacy of the data during collection, processing and transmission. Allow access of the data only to authorised entities
- Use a lightweight, memory and energy-efficient cryptographic algorithm for encryption
- Facilitate a key management service for key generation, key refreshing, key agreement, key distribution and key revocation
- Include a firewall and intrusion detection system to identify and block suspicious activity on a network
- Include proper logging techniques for auditing and accountability
- Include data backup strategy to assure high availability of the application
- Assure physical protection of all identified assets

After identifying the security and privacy requirements below two tasks need to be conducted:

- Update the initial product requirements with security and privacy requirements
- Document the security and privacy requirements in the security assessment report

4.1.4 Risk assessment at the system architecture phase

The objective of conducting a risk assessment at the system architecture phase is to review the system architecture, identify the security and privacy risks, evaluate the identified security and privacy risks, apply risk treatment to identify the security and privacy risks which will require controls to mitigate and update the security and privacy requirements. The updated product requirements, system architecture and risk assessment approach will be taken as an input to this phase. Figure Appendix B- 6 illustrates the steps to conduct a security and privacy risk assessment at the system architecture phase.

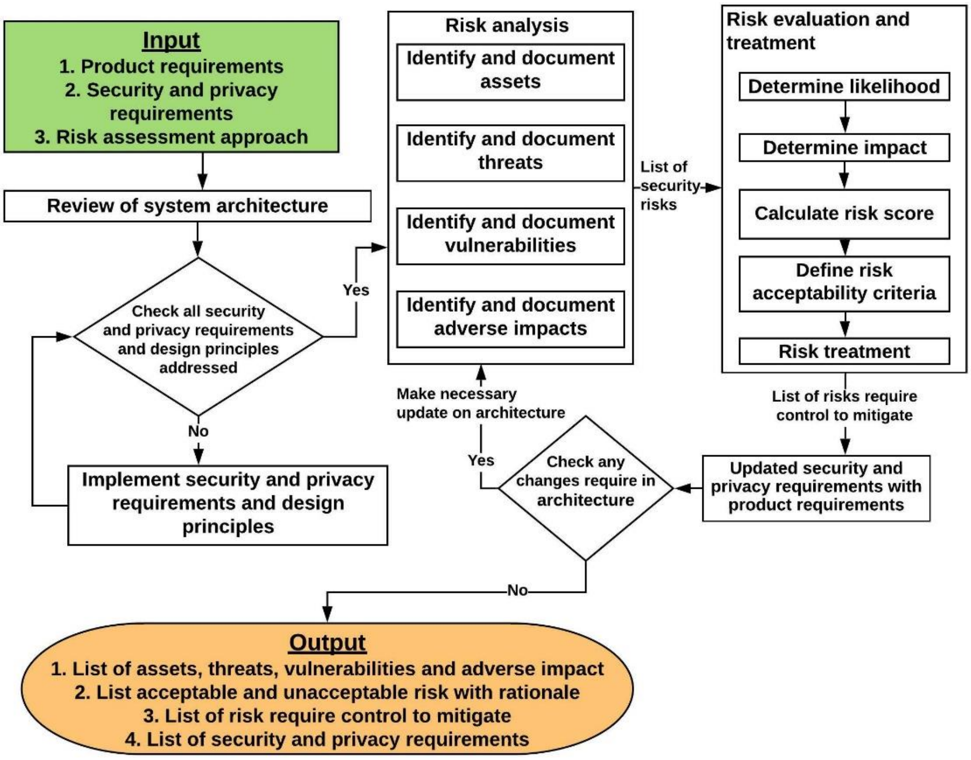

Input
1. Product requirements
2. Security and privacy requirements
3. Risk assessment approach
Review of system architecture
Check all security and privacy requirements and design principles addressed
Yes
No
Implement security and privacy requirements and design principles
Risk analysis
Identify and document assets
Identify and document threats
Identify and document vulnerabilities
Identify and document adverse impacts
List of security risks
Risk evaluation and treatment
Determine likelihood
Determine impact
Calculate risk score
Define risk acceptability criteria
Risk treatment
List of risks require control to mitigate
Updated security and privacy requirements with product requirements
Check any changes require in architecture
Yes
Make necessary update on architecture
No
Output
1. List of assets, threats, vulnerabilities and adverse impact
2. List acceptable and unacceptable risk with rationale
3. List of risk require control to mitigate
4. List of security and privacy requirements

Figure Appendix B- 6: Risk assessment steps in the system architecture phase

Below is the list of key tasks that will be conducted during the security and privacy risk assessment at the system architecture phase:

- Review system architecture according to security principles and security and privacy requirements identified in section 4.1.3.3
- Apply security and privacy risk analysis to identify the security and privacy risk
- Evaluate each security and privacy risk to identify acceptable and unacceptable risks
- Apply security and privacy risk treatment to identify the list of unacceptable security and privacy risks which will require security and privacy controls to mitigate
- Update security and privacy requirements and product requirements with unacceptable risks
- Check whether any update to the current system architecture is required due to newly identified security and privacy requirements. If yes, then make necessary changes to

the system architecture and conduct risk analysis followed by risk evaluation and treatment.

The rest of the section is organised as follows; section 4.1.4.1 provides guidance on designing and reviewing the system architecture. Section 4.1.4.2 provides guidance on identifying security and privacy risks by conducting risk analysis while section 4.1.4.3 details steps to evaluate and create a treatment plan for security and privacy risks. Finally, section 4.1.4.4 outlines the list of security and privacy requirements that need to be taken into consideration.

4.1.4.1 Review system architecture

The system architecture is a conceptual representation of relationships and interactions between various elements required to develop the application. During the system architecture review, an organisation needs to consider the following three steps:

- Review the system architecture for compliance with architecture security design principles. To review system architecture, organisations should take the following design security principles into consideration:
  - Identify whether each component of the application will interface externally or internally or both
  - Identify how the user will access each component of the application and define the trust boundary of user access
  - Define the trust boundary while interfacing each component
  - Use least privilege principle while accessing and interfacing any component
  - The threats and vulnerabilities identified in the requirement analysis phase take in considerations while designing the security capabilities

  - Identify the use of any third-party components and their security capabilities that will be used to develop the application
  - Define the software technology stack at the application level
  - Define the programming technology that will be used to develop the application
  - Keep the system architecture as simple as possible

- Review the system architecture to assure that all security and privacy requirements identified in section 4.1.3.3 are implemented
- Upon review of the system architecture check all security and privacy requirements and security design principles are implemented properly. If any security and privacy requirements and design principles are not implemented, then implement the missing one and iterate the review process.

4.1.4.2 Security and privacy risk analysis

To conduct risk analysis in system architecture phase, the following four steps need to perform. Among these four tasks, identifying the threats and vulnerabilities steps can be performed in any order.

1) **Identify and document the assets:** To identify and document the assets in the system architecture, the assessor team should conduct the following steps:
    a. Check whether any new asset is discovered compared to the list of assets identified during the requirement analysis phase in section 4.1.3.1
    b. Document the complete list of assets with newly discovered (if any) in the risk assessment report
2) **Identify and document the threats:** To identify and document the threats at the system architecture phase, the assessor team should conduct the following steps:

a. Follow the steps outlined in section 4.1.3.1 to identify the threats

b. To identify threats for any new assets identified at the architecture phase, the assessor team should consider the following steps:

   i. If the asset is available in Table Appendix E-1 in Appendix E, then get the respective threat name from the list

   ii. If the asset is not available in Table Appendix E-1 in Appendix E, then get the respective threat from an external sources such as research articles, blog posts, open-source platforms such as OWASP[9], governmental agencies such as US-CERT[10], European Union Agency for Cybersecurity (ENISA)[11] and NIST[12].

c. Document the complete list of threats, including newly discovered threats (if any), in the risk assessment report

3) Identify and document the vulnerabilities: To identify vulnerabilities at the system architecture phase, the assessor team should conduct the following steps:

a. Apply an attack tree or threat modelling approach. STRIDE and LINDDUN are the most suitable threat modelling methods. Section 2.4.2 under Appendix D outlines guidance on how to conduct threat modelling based on STRIDE methodology and use attack trees to identify vulnerabilities in a WBAN application

[9] https://owasp.org/www-community/attacks/

[10] https://www.us-cert.gov/resources/cybersecurity-framework

[11] https://etl.enisa.europa.eu/

[12] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

b. Check if there are any additional vulnerabilities to those in the list of vulnerabilities identified during the requirements analysis phase in section 4.1.3.1

c. If yes, then record the newly discovered vulnerabilities with description and possible countermeasure (if available) in the security assessment report

4) **Identify and document the adverse impacts:** To identify the adverse impact of newly discovered threats and vulnerabilities, the assessor team can reuse the questionnaire and process outlined in the requirement analysis phase (see section 4.1.3.1).

4.1.4.3 Risk Evaluation and treatment

To identify the treatment for the security and privacy risks identified at the system architecture phase, the team should follow the steps outlined in section 4.1.3.2. There now follows a summary of the steps that need to conduct to complete a risk evaluation and treatment at the system architecture phase:

- Follow the steps outlined in section 4.1.3.2 to determine the impact of threats and vulnerabilities
- Follow the steps outlined in section 4.1.3.2 to determine the likelihood of threats and vulnerabilities
- Follow the steps outlined in section 4.1.3.2 to calculate the risk score
- Follow the steps of risk acceptability criteria outlined in section 4.1.3.2 to identify the acceptable and unacceptable security and privacy risks
- Follow the steps of risk treatment outlined in section 4.1.3.2 to identify the list unacceptable risk which will require security and privacy risk control to mitigate

- Finally, document the updated product requirements, list of acceptable and unacceptable risk along with risks that require security and privacy risk controls for mitigation, in the risk assessment report.

4.1.4.4 Update security and privacy requirements

Follow the steps outlined in section 4.1.3.2 to develop the security and privacy requirements for the unacceptable risks which require controls to mitigate. Update the product requirements with the updated security and privacy requirements. If the updated security and privacy requirements require modifications to the system architecture, then conduct the following steps:

- Make necessary modifications to the system architecture
- Iterate the risk analysis and security and privacy evaluation with treatment process until the security and privacy requirements are addressed in the system architecture.

4.1.5 Security and privacy risk assessment report

The result of the security and privacy risk assessment needs to be documented in a report. The report should include the following properties:

- Scope of the risk assessment
- Team members who conducted the risk analysis and date
- Team members who conducted the security and privacy risk evaluation and treatment with date
- Initial product requirements
- Selected risk assessment approach with rational
- List of assets identified in the requirements analysis and the system architecture phase

- List of threats and vulnerabilities, along with their description, impact and likelihood score that were identified in both the requirement analysis and the system architecture phase
- The adverse impact of each threat and vulnerability identified at both the requirement analysis and the system architecture phase
- Risk acceptability criteria with rationale for both the requirements and system architecture phases
- List of acceptable security and privacy risks with rational
- List of unacceptable security and privacy risks
- List of unacceptable security and privacy risks to be shared or avoided
- List of unacceptable security and privacy risks which require controls to mitigate
- List of security and privacy requirements identified at both the requirement analysis and the system architecture phase

4.2 Security and Privacy Risk Controls

Security and privacy risk controls are safeguards or countermeasures whose purpose is to mitigate the threats and vulnerabilities to an application. The effectiveness of the control will depend on the circumstances, the business goals, the types of hardware and software components and their failure modes, and on the criticality of the specific requirements for the application. Organisations should form a team to identify the security and privacy risk controls to mitigate the unacceptable risks which require controls for mitigation. An organisation should include all assessment team members as presented in Table Appendix B- 1. The team is comprised of the product owner, project manager, technical lead, senior software engineer, developer, QA engineer and QA team. The purpose of this stage is to select, implement and verify security and privacy risk controls. This stage will take a list of unacceptable risks which require security and privacy controls to mitigate as the input and produce an application that has all the necessary security and privacy risk controls implemented and verified. Figure Appendix B- 7 presents the steps for the selection and implementation of control to mitigate the unacceptable risks.

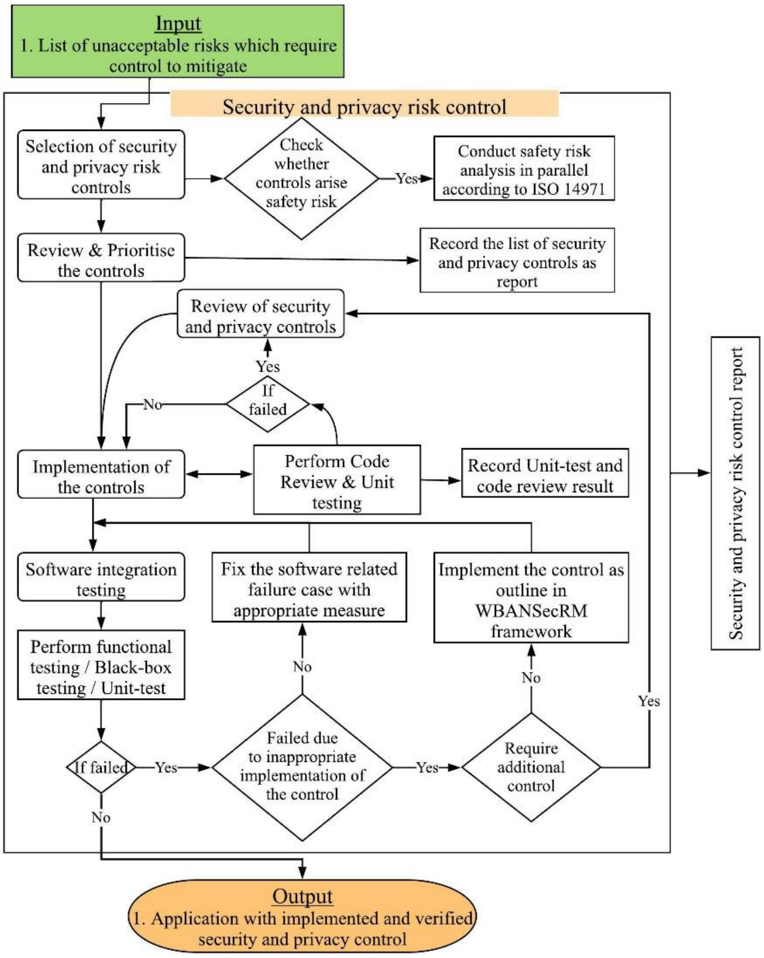

Input
1. List of unacceptable risks which require control to mitigate
Security and privacy risk control
Selection of security and privacy risk controls
Check whether controls arise safety risk
Yes
Conduct safety risk analysis in parallel according to ISO 14971
Review & Prioritise the controls
Record the list of security and privacy controls as report
Review of security and privacy controls
Yes
If failed
No
Implementation of the controls
Perform Code Review & Unit testing
Record Unit-test and code review result
Software integration testing
Fix the software related failure case with appropriate measure
Implement the control as outline in WBANSecRM framework
Perform functional testing / Black-box testing / Unit-test
No
No
Yes
If failed
Yes
Failed due to inappropriate implementation of the control
Yes
Require additional control
No
Security and privacy risk control report
Output
1. Application with implemented and verified security and privacy control

Figure Appendix B- 7: Selection and implementation process of security and privacy risk control

The remainder of this section is organised as follows; section 4.2.1 provides guidance on how to select appropriate risk controls followed by section 4.2.2 provide guidance to identify risk arising from risk controls. Section 4.2.3 details how to prioritise the risk controls. Following this, section 4.2.4 details the steps to implement the controls and verify the implementation of controls by conducting code review and unit testing. Section 4.2.5 outlines the criteria for reviewing the risk control. Section 4.2.6 outlines the steps to conduct software integration testing. Finally, section 4.2.7 details what needs to be included in the security and privacy risk control report.

4.2.1 Selection of security and privacy risk controls

The aim of this stage to identify security and privacy risk controls to mitigate threats and vulnerabilities. Below are the steps that should be conducted in order to select the appropriate security and privacy risk controls:

1. Select the recommended controls for each threat and/or vulnerability presented in Table Appendix E-1 under Appendix E
2. If the threat and/or vulnerability is not listed in Table Appendix E-1 under Appendix E, then follow steps 2a and 2b to identify the controls;
    a. If a threat or a vulnerability was identified from external sources such as OWASP, NIST, ENISA and US-CERT, then check these external sources for *"Related Controls"*, or *"Potential Mitigations"* or read their respective description to identify the possible countermeasure for that threat and/or vulnerability
    b. If a threat or vulnerability was identified using any threat modelling tools, then check the description provided by the threat modelling tool for possible countermeasures

Additionally, it is essential to check whether any of the selected controls can give rise to any safety-related risks. As the goal of this framework is only to identify and mitigate the security and privacy related risk, the organisation need to separately conduct safety risk analysis by using guidelines provided by ISO 14971 (BSI, 2009) to mitigate the safety related risks.

Finally, document each security and privacy risk control along with the respective threat and vulnerability name in the security and privacy risk control report.

4.2.2 Risks arising from risk control measures

The organisation should seek to balance usability, device safety, and device security and privacy to assure that the controls are appropriate for the intended users and any systems to which the device is connected. Related decisions and trade-offs should be documented. It is possible that new risks of harm could be unintentionally added to the system due to the implementation of the controls. For example, use of password authentication which adds unacceptable delay in accessing the device during an emergency. Each proposed risk control should be analysed for the potential of introducing new safety, security and privacy risks.

4.2.3 Review and prioritise the security and privacy risk controls

After completing the security and privacy risk control selection process, the next task is to review the implementation details of each control and prioritise them. The review and prioritisation of the security and privacy risk controls should be conducted as follows:

- A team, comprised of a technical lead, a developer, and a QA person will review the implementation details presented in Appendix C for each of the security and privacy risk controls
- Gather initial understanding of the resources required to implement the control
- Prioritise the security and privacy risk controls based on below factor:
    - Risk score level
    - Product delivery plan and timeline of the project
    - Go to market plan
    - The priority of each use case

    - Complexity, time and resources required to implement each security and privacy risk control

- Alternatively, use expert consensus to prioritise the security and privacy risk control based on the relationship between multiple risks mitigate by one or more control
- Upon completion of the review and control prioritisation, the list of selected controls, along with their respective implementation details and prioritisation, should be documented in the security and privacy risk control report
- Finally, handed over the list of selected controls along with their respective implementation details and prioritisation to the development team for implementation

4.2.4 Implementation and verification of security and privacy risk controls

In the development phase, the developer will implement and verify each of the selected security and privacy controls. During the implementation of the security and privacy risk control, developers should consider secure coding practices. Secure coding practices help reduce the chance of introducing unwanted vulnerabilities during development. The developer will use organisation defined secure coding practices if available; otherwise the developer can follow the secure coding guidelines provided below. Finally, to verify whether controls have been implemented properly, code review and unit testing should be conducted followed by usability testing using the guidelines provided by IEC 62366.

Secure coding guidelines:

- Validate input from all data sources
- Compile code using the highest warning level available in the compiler and take necessary action to resolve the warnings
- Use version controlling to track changes made to the code

- Sanitise the input to SQL statements. Use parameterised SQL statements. Do not use string concatenation or string replacement to build SQL statements.
- Use the latest version of compilers, which often include defences against coding errors; for example, GCC protects code from buffer overflows
- Include proper error/exception handling. Check the return values of every function, especially security-related functions. Also, check for leakage of sensitive information to untrusted users
- Encode HTML input field data. Attackers use malicious input to conduct XSS attacks. Encoding of every user-supplied input can prevent the client's web browser from interpreting these as executable code. Do not store sensitive data in cookies
- Encrypt all confidential data using strong cryptographic techniques. Use a published and strong cryptographic algorithm with a sufficiently long key
- Use code analysis tools to find security issues early

Code Review: Code review is an effective technique to examine the source code to minimise the coding error and reducing the risk of vulnerability exposure during the implementation phase of software development. Secure coding guidelines also need to be considered during the code review process. Code review can be performed manually and/or by using an automated tool. To conduct a manual code review, organisations need to assign an experienced person from the development team. To conduct a code review using an automated tool, an organisation needs to select the tool based on the technology stack. There are various automated code review tools available such as; SonarQube, IBM Security AppScan, Code Dx or Veracode which support a wider range of technology stacks.

Unit Testing: Unit testing is a testing method which helps to test an individual unit or components of an application. The goal of unit testing, from a security perspective, is to verify that each implemented control effectively mitigates its respective security and privacy risk. Usually, the unit test case is written by a developer with the help of the QA team. Sample acceptance criteria for unit-tests are present in Table Appendix B- 9: . The example below details the test to verify that the countermeasure for "*Weak Authentication Scheme*" is properly implemented.

Sample use case: *User login with username and password*

Test objectives: *Verify that the identity requirements for user authentication are aligned with business and security and privacy requirements*

Sample acceptance criteria for unit-test:

Table Appendix B- 9: Sample acceptance criteria for Unit testing

ID	Test case	Expected result
TEST01	Testing for Valid user/right password	Successful authentication response
TEST02	Testing for valid user/wrong password	Authentication failed due to the wrong password
TEST03	Testing for a nonexistent username	Authentication failed due to invalid username
TEST04	Testing authentication with blank passwords	Authentication failed due to empty password supplied
TEST05	Attempt to log in with an incorrect password four times	Account locked out due to maximum try with the wrong password. Please contact the administrator.

If the code review or unit test identifies any security and privacy control failures, then the developer needs to conduct the following steps in order:

- Review the reason of the failure based on the scenario presented in section 4.2.5
- Take necessary action to address the failure case as described in section 4.2.5
- Conduct code review and/or unit test again to check whether the failure case is addressed

Finally, the result of the code review and the unit testing needs to be documented in the security and privacy risk control report with the updated list of controls (if any new control were added).

4.2.5 Review of security and privacy controls

The aim at this stage is to present a list of reasons which can cause a security and privacy control to fail. During the review of the control failures, the following considerations need to be taken into account in order to identify the root cause of the failure:

- The control was not properly implemented according to the implementation guidelines outlined in Appendix C. In that case the developer needs to implement the control again according to the implementation guidelines
- Appropriate security and privacy risk control was not selected for addressing the threats and/or vulnerabilities. If the appropriate control is not available in Appendix C then analyse external sources such as NIST 800-53, ISO 27005, OWASP, Autodesk continuous threat modelling developer checklist[13] and blogs or appropriate control and implantation details
- The developer did not follow appropriate secure coding practices during implementation of security and privacy risk control

4.2.6 Software integration testing

Software integration testing is a level of software testing where individual units are combined and tested as a group. Integration tests help to identify whether independently developed units of software work correctly when they are connected to each other. Integration testing can adopt different approaches, such as; Black Box Testing, White Box Testing and Gray Box Testing methods. During software integration testing, the developer needs to conduct two key tests:

[13] https://github.com/Autodesk/continuous-threat-modeling/blob/master/Secure_Developer_Checklist.md

- Security and privacy requirements testing - to validate the security and privacy requirements identified during the risk assessment steps are implemented properly. This can be achieved by conducting functional, performance and scalability testing
- Threat and vulnerabilities mitigating testing - to validate the effectiveness of the implemented controls against the identified threats and vulnerabilities

The following steps should be conducted in the software integration testing stage:

- Perform integration testing by conducting functional testing, unit-test, black-box, white box, and gray box testing. Organisations can use one or a combination of multiple testing approaches to conduct the integration testing based on the QA resource expertise and availability.

  Example integration test cases for WBAN application:

  - Verifying the interface link between the login page and the home page, i.e. when a 'User' enters their credentials and logs in, they should be directed to the homepage
  - Verifying the interface link between the home page and the profile page, i.e. profile page should open up
  - Verifying the interface link between the home page and device page on the mobile app i.e. device page should open up and show connected sensor devices
- If an integration test fails, then check whether it failed due to inappropriate implementation of the security and privacy risk control
  - If no, then take appropriate measures to fix the software related failure case and conduct the software integration test again
  - If yes, then check whether any additional controls are required. If yes, then review the security and privacy controls based on considerations presented in

section 4.2.5 of Appendix B. If no, then implement the security and privacy control as outline in Appendix C and conduct the software integration test again

4.2.7 Security and privacy risk control report

Finally, the result of the security and privacy risk control needs to be documented in a report. The report should include the following properties:

- List of selected security and privacy risk controls with their implementation details
- Prioritisation of security and privacy risk controls
- List of tools used for code review
- List of unit test cases for each security and privacy risk control
- Result of code review and unit-testing with list of actions taken to address if code review and/or unit test failed
- List of tools and testing methods used for software integration testing
- Result of software integration testing
- List of actions taken if the software integration test failed

4.3 Evaluation of Overall Residual Security and Privacy Risk Acceptability

Upon completion of the security and privacy risk control implementation and verification stage, the overall residual security and privacy risk needs to be assessed. Evaluating an application's overall residual security and privacy risk is a complex process as determining how an attacker will exploit the application and the severity level of the exploit, is difficult to assess. According to the TIR 57 standard, an organisation can employ security testing techniques such as vulnerability scans and/or penetration testing to assess the overall residual security and privacy risk of an application. Additionally, organisation can also conduct assessment of the system security configuration and hardening configuration files to mitigate the possible vulnerabilities.

This stage will take the application with security and privacy risk controls implemented and verified as input to conduct the vulnerability scans and/or penetration testing. The organisation should form a team to perform security testing, as presented in Table Appendix B- 1. The team is comprised of the product owner, project manager, technical lead, software architect, senior software engineer and third-party resources (if required) such as penetration testers. Figure Appendix B- 8 presents the steps for evaluating the overall residual security and privacy risk of the application.

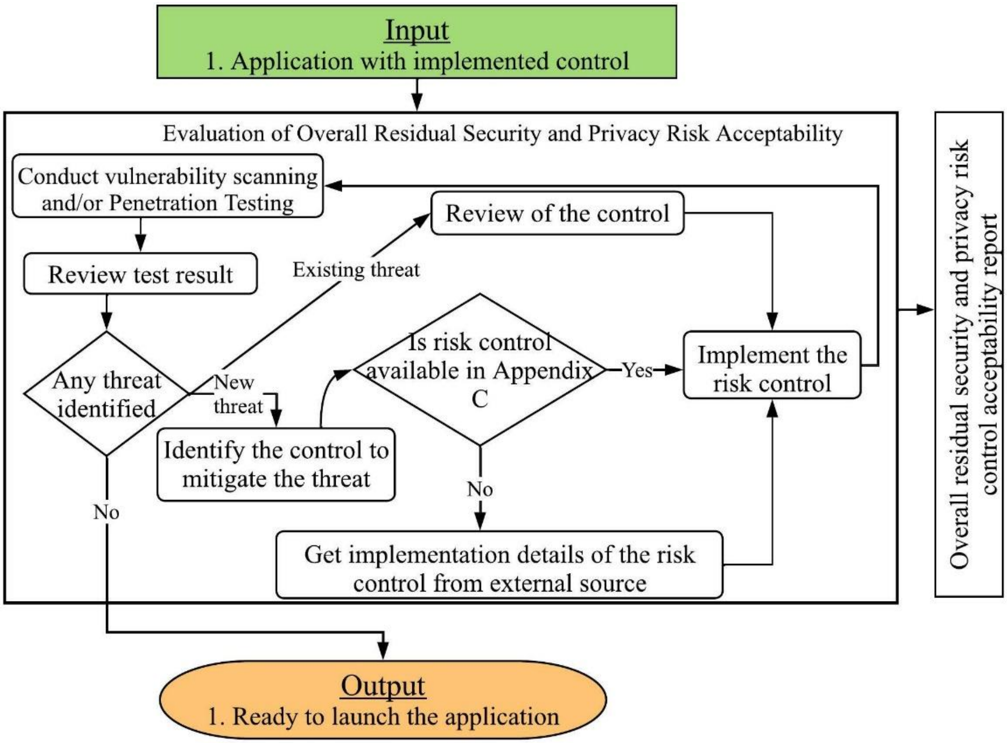

Input
1. Application with implemented control
Evaluation of Overall Residual Security and Privacy Risk Acceptability
Conduct vulnerability scanning and/or Penetration Testing
Review of the control
Review test result
Existing threat
Any threat identified
New threat
Is risk control available in Appendix C
Yes
Implement the risk control
Identify the control to mitigate the threat
No
No
Get implementation details of the risk control from external source
Overall residual security and privacy risk control acceptability report
Output
1. Ready to launch the application

Figure Appendix B- 8: Steps for evaluating the overall residual security and privacy risk acceptability

The remainder of this section is organised as follows; section 4.3.1 provides guidance for conducting vulnerability scanning and/or penetration testing. Section 4.3.2 details the steps to review the test results and take necessary actions to mitigate if any additional threats are identified. Finally, section 4.3.3 details what needs to be documented.

4.3.1 Conduct vulnerability scanning/penetration testing

Vulnerability scans and penetration testing are very different from each other, but both serve important functions for evaluating the implemented security and privacy risk controls. An overview of vulnerability scanning and penetration testing, and possible tools that can be used to conduct this testing, is presented below.

Vulnerability scanning: A vulnerability scan only discovers known vulnerabilities; it does not attempt to exploit a vulnerability but instead only confirms the possible existence of a vulnerability. An organisation can conduct vulnerability scanning using an automated tool with some manual support. Table Appendix B- 10 illustrates the list of possible tools for vulnerability scanning. A vulnerability scan is a very quick, cost-effective way to perform testing and can be made an automatic process for periodic testing using an automatic tool. The limitation of vulnerability scanning is that it only scans for known vulnerabilities, provides a list of possible vulnerabilities and does not confirm whether those vulnerabilities are exploitable or not.

Table Appendix B- 10: List of tools for vulnerability scanning

Name	Description	License	Source
OpenVAS	OpenVAS Scanner is a vulnerability assessment tool that is used to spot issues related to security in the servers and other devices of the network.	GNU General Public License	[Link]
Nikto	Nikto is an open-source web scanner employed for assessing the probable issues and vulnerabilities on web servers.	GNU General Public License	[Link]
Tripwire IP360	Tripwire IP360 is a vulnerability assessment solution to run wide-ranging of testing on the networks to spot all the vulnerabilities, configurations, applications, network hosts.	Commercial	[Link]
Wireshark	Wireshark is an extensively used as network protocol analyser tool.	GNU General Public License	[Link]
Aircrack	Aircrack is a tool to assess the WiFi network security.	GNU General Public License	[Link]

Penetration testing: Penetration testing is a security testing approach which identifies exploitable vulnerabilities of a system, or of individual components of a system. Penetration testing helps to replicate the adversary’s actions in carrying out attacks against the application and provides an in-depth analysis of security and privacy-related weaknesses or deficiencies. Penetration testing requires specialised skills, higher budgets and more time than vulnerability scanning. An organisation can conduct penetration testing by forming a team of people within the organisation who have the technical expertise to conduct a penetration test. If an organisation does not possess the required expertise, they can on-board external resources with the required expertise to conduct penetration testing. Table Appendix B- 11 illustrates the list of possible penetration testing tools.

Table Appendix B- 11: List of tools for penetration testing

Name	Description	License	Source
Apache ab test	Apache ab load test tool uses to generate the number of request per second. This tool very useful to perform load testing and DDOS attack scenario.	GNU General Public License	[Link]
OWASP ZAP	The Open Web Application Security Project - Zed Attack Proxy (ZAP) is a penetration testing tool for finding vulnerabilities in applications.	GNU General Public License	[Link]
BURP SUITE	Burp Suite is a platform for performing security testing of applications.	Commercial	[Link]
NMAP	Nmap (Network Mapper) is a free and open-source utility for network exploration or security auditing.	GNU General Public License	[Link]
SSLSCAN	SSLScan tests for different SSL exploits, such as heartbleed and the POODLE vulnerability, it also tests the cipher suites and key exchanges.	GNU General Public License	[Link]
HYDRA brute force	Hydra is a rapid dictionary attacker which can be configured against over 50 different protocols. It is most commonly used for brute-forcing user accounts to test for weak passwords.	GNU General Public License	[Link]
KALI LINUX	Kali is a Debian-derived Linux distribution designed for digital forensics and penetration testing installed with hundreds of different tools.	GNU General Public License	[Link]

Organisation can use below criteria to select the appropriate method for evaluating the overall residual security and privacy risk of the application:

- Choose penetration testing as it will provide a very high level of assurance and in-depth testing of the implemented controls
- Choose only vulnerability scanning if the application only records a limited amount of parameters without personally identifiable information

- Choose both penetration testing and vulnerability scanning if time and budget allow

To conduct vulnerability scanning and/or penetration testing, an organisation should conduct the following steps:

- Define the scope of the vulnerability scanning and/or penetration testing. The scope will include:
    - List of application use-cases
    - List of assets
    - List of threats and vulnerabilities for which countermeasures are implemented
- Select the tools to be used to conduct the vulnerability scanning and/or penetration testing
- Include external expertise (if required) for conducting the scanning and/or testing
- Collect the result of vulnerability scanning and/or penetration testing for review
- Document the scanning and/or test report in overall residual security and privacy risk acceptability report including:
    - Date of the vulnerability scanning and/or penetration testing
    - Name of people/organisation who performed the scanning and/or testing
    - Scope of the scanning and/or testing
    - List of tools used for conducting scanning and/or testing

4.3.2 Review test result

After conducting the vulnerability scanning and/or penetration testing, the results of the testing need to be reviewed. Passing a penetration test/vulnerability scanning does not guarantee that the application is invulnerable, however it does mean that the application is at least invulnerable within the scope of the testing. If the vulnerability scanning and/or penetration testing are successful (i.e. do not record a fail), then the organisation can mark the product for launch. If the testing/scanning fails, then the root cause of the failure needs to be analysed. To conduct the analysis, the following steps should be followed:

- Check whether the threat is a new threat or existing threat which was identified during the security and privacy risk assessment at the requirements and system architecture phase
- If the threat is an existing threat, then perform a review of the security and privacy risk controls based on the considerations presented below:
    - The security and privacy control were not properly implemented according to the implementation guidelines outlined in Appendix C. In that case the developer needs to implement the security and privacy control again according to the implementation guidelines
    - Appropriate security and privacy risk control was not selected for addressing the threats and/or vulnerabilities
    - The developer did not follow appropriate secure coding practices during implementation of security and privacy risk control

  When the cause of the failure is identified, take appropriate measures to address the failure case and mitigate the identified threat
- If the identified threat is a new threat, then check whether the suggested security and privacy risk control is available in Appendix C
    - If yes, then implement according to implementation details to mitigate the threat and add the selected security and privacy risk control to the existing list
    - If no, then collect implementation details from external sources such as; NIST 800-53, ISO 27005, OWASP, blogs etc. Update the existing implementation

details list in Appendix C with the newly identified threat and respective security and privacy risk control with implementation guidelines

- Upon completion of the implementation of the security and privacy risk control, testing/scanning needs to be conducted again to verify that the control successfully mitigates the identified threat
- Document the action taken to address each threat in the overall residual security and privacy risk acceptability report

4.3.3 Overall residual security and privacy risk acceptability report

Finally, the result of the evaluation of the overall residual security and privacy risk needs to be documented in a report. The report should include the following properties:

- Scope of vulnerability scanning and/or penetration testing
- Team members including third-party resources (if on-boarded) who conducted the vulnerability scanning and/or penetration testing and date when the scanning/testing is performed
- List of tools used for vulnerability scanning and/or penetration testing
- List of threats (if identified from vulnerability scanning and/or penetration testing)
    - List of security and privacy risk controls implemented to address the threats
    - List of security and privacy controls with implementation details collected from external sources

Appendix C Implementation Guideline for Security and Privacy Controls

Access Control:

To avoid the unauthorised access to data, an access control policy needs to be in place. Below is the list of controls selected from different capabilities of ISO/IEC 80001-2-8 standard to achieve proper access control.

Source:

NIST 800-53 r5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-7, AC-9, AC-10, AC-17

ISO IEC 27002 / ISO 27799: 9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.1, 9.4.5

Guidelines:

- Access Control Policy:
    - Develop an access control policy which will address purpose, scope, roles, responsibilities and consistent with regulations (AC-1, 9.1.1)
    - Define and document the types of system accounts allowed for use within the system in support of organisational missions and business functions (AC-2)
    - Specify authorised users of the system, group and role membership, privileges for each account (AC-2)
    - Provide physical or logical access controls for the isolation of applications, application sensitive data, or systems (AC-3, 9.4.1)
    - Assign account managers for managing system accounts (AC-2)
- Automatically disable the account when the account is expired, no longer associated with a user or used by the application (AC-2)

- Notify account managers when an account no longer required, or user is no longer is using the application (AC-2)
- Implement role-based, attribute-based access with proper access level for application (AC-3)
- Define the authorisation access based on the duties of individuals or user (AC-5)
- Perform periodic review of access rights, reassign or revoke privilege if necessary (AC-6, 9.2.5, 9.2.6)
- Enforce a limit of consecutive invalid login attempts by a user during a period. Automatically lock the account when the maximum number of unsuccessful log-on attempts is exceeded (AC-7)
- Notify the user upon unsuccessful login/access attempts since the last successful login/access. Include additional information such as; date-time, location for last login attempt (AC-9)
- Assure that user access to the application is not activated before authorisation procedures are completed (9.2.2)
- If applications or device provide default password or temporary secret authentication information for the user, force user to change this during first-time log-on (9.2.4)
- Temporary secret authentication information should be unique for each user and should not be guessable (9.2.4)
- Assign a unique ID for each user and attached appropriate access rights with that ID (9.2.3)
- Use centralised access management to manage access privileged (9.2.2)
- Limit the number of concurrent sessions for each user while accessing the application (AC-10)

- Authorise remote access to the system before allowing such connections communicating through external network (AC-17)
- Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions (AC-17)
- Access to the application program source code should be restricted (9.4.5)
- Updating of program source code and associated libraries should only be performed by an authorised user (9.4.5)
- Maintain an audit log for all access to program source code (9.4.5)
- Revoke user and/or device access to the application if compromised, provide alternative approaches if immediate revocation is necessary (AC-3)

Authentication and Authorisation:

Authentication and authorisation processes are required to identify that a request originated from a trustworthy source or user. Below is the list of guidelines selected form various controls presented in ISO/IEC 80001-2-8 standard. As this standard does not provide any guidelines for creating a strong password, so OWASP authentication guidelines are used to create a strong password (OWASP Authentication). Once user is successfully authenticated by the application, it is desirable that user continue using the application without re-authenticated within a certain period. So, proper session management is required to support this feature. RFC 6749 guidelines are used for session management using access token (6749, no date).

Source:

NIST 800-53 r5: AC-7, AC-11, AC-12, IA-2, IA-3, IA-5, IA-11

ISO IEC 27002 / ISO 27799: 9.2.1, 9.4.2, 9.4.3

OWASP Authentication guidelines

RFC 6749 - The OAuth 2.0 Authorization Framework

Guidelines:

- Implement a formal user registration and de-registration process with a unique user ID (9.2.1)
- If possible, implement multifactor authentication for both server access and application access (*IA-2*)
- Implement device identification and authentication process (specified by organisation) before providing access to the application (IA-3)
- Lock user accounts after a certain number of failed logins attempts during a time-period (AC-7)
- Retain the device lock until the user re-establishes access using re-authentication procedures (AC-11)
- Implement automatic log-off from the application if the user is inactive for a certain period (AC-12)
- Do not display a password being entered (9.4.2)
- Do not transmit passwords in clear text over a network (9.4.2)
- Enforce input validation for an email address and password (OWASP)
- Maintain a record of previously used passwords and prevent re-use (9.4.3)
- Validate email address by sending the email verification link (OWASP)
- Email verification link must expire after the first use or expire after 8 hours (OWASP)
- Enforce user to create a strong password by using below policy (OWASP):
    - A minimum length of 8 characters

  - Must not contain significant portions (three or more contiguous characters) of your account name or full name
  - A mix of upper-case characters, lower case characters, and numbers or special characters must contain characters from at least three of the following four categories arranged in any order
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters: ~!@#$%^*&;?.+_
  - Not more than two identical characters in a row
- Maintain a list for commonly used, expected, or compromised passwords and update the list when passwords are compromised directly or indirectly (IA-5)
- When users create or update passwords verify that passwords are not found on the list of commonly used, expected, or compromised passwords (IA-5)
- Enforce user to re-authenticate when device or account lock, role privileged changes (IA-11)
- Session management using access token (RFC 6749):
  - Use session-based JWT access token using OAuth for authentication
  - Generate a new access token every time user request for login
  - Use strong encryption like SHA-256 or AES-128 for storing the access token
  - Set short expiry time for the access token, expiry time can be 30 mins or one hour
  - Refresh session-based token before the access token is expired

  - Use the “state” parameter to link authorisation request with redirect URI used to deliver a session-based token
  - Do not pass oAuth2.0 tokens in page URLs
  - Use “*jti”* field to provide a way to blacklist tokens that have been used more than X times (perhaps even a user)
  - Use Authorization headers or POST parameters instead of URI request parameters

Physical Protection:

Implement proper safeguard to assure physical protection of sensor node, including storage area and physically tamper prevention and detection. Sensor node storage area including removable hard drive, flash drive.

Source:

NIST 800-53 r5: MP-4, PE-3, SA-18, SC-28

ISO IEC 27002 / ISO 27799: A.11.2.7

Guidelines:

- Implement automated mechanisms to restrict access to the media storage area of sensor node and audit access attempts (MP-4)
- Employ security safeguards for physically tampering or alteration by implementing tamper detection and prevention within the sensor node device. Tamper-detection seals and anti-tamper coating can be used for tamper detection and prevention (PE-3, SA-18)

- Implement cryptographic mechanisms to prevent unauthorised disclosure and modification of data while residing in sensor device. Use encrypted storage device or encrypt all information on storage area (SC-28)
- All storage media area containing confidential information need to securely destroy before disposal or re-use of sensor device. Information from the storage media area need to destroy or overwritten in such way so that original information become non-retrievable (11.2.7)

Client Platform Security:

Protect client handheld device storage area such as; removable hard drive, flash drive. Implement malicious code protection and malware detection to keep safe the device from the attacker.

Source:

NIST 800-53 r5: MP-4, SC-28, SI-3

ISO IEC 27002 / ISO 27799: 6.2.1

Guidelines:

- Implement automated mechanisms to restrict access to the media storage area of client handheld device and audit each access attempts (MP-4)
- Implement cryptographic mechanisms to prevent unauthorised disclosure and modification of data while residing in the client handheld device. Encrypt all information or specific data structure including files, records, or fields on storage area (SC-28)

- Implement signature-based or non-signature based malicious code protection mechanisms at system entry and exit points to detect and remove malicious code. Perform periodic scans from external sources and send alert to administrator in response to malicious code detection (SI-3)

Cryptography and Encryption:

Protect the confidentiality and integrity of data during transmission and reside at rest. Unprotected communication paths are exposed to the possibility of interception and modification of data. Encryption technique needs to use for assuring data confidentiality and integrity. As NIST 800-53 does not provide any guidelines for cryptographic algorithm selection. So, NIST 800-175B standard use for cryptographic algorithm selection.

Source:

NIST 800-53 r5: SC-8, SC-17, SC-28

ISO IEC 27002 / ISO 27799:

NIST 800-175B

Guidelines:

- Encrypt data to prevent unauthorised disclosure of information, detect changes to information during transmission (*SC-8)*
- Implement cryptographic mechanisms to prevent unauthorised disclosure and modification of data while residing data at rest (SC-28)
- Implement cryptographic mechanisms including hash function, digital signatures, checksums and message authentication code to protect information integrity (*SC-8)*

- Implement cryptographic mechanisms to protect message externals such as; message headers and routing information (*SC-8)*
- Issue public key certificates for transmission from an approved service provider (SC-17)
- Do not use any random cryptographic algorithms. Select only those cryptographic algorithms which are recognised by different standard. For example; AES currently recognise by Federal Government standard body for symmetric techniques (NIST 800-175B)
- Consider the proper key size during cryptographic algorithms. For AES 128, 168 or 256-bits key size can be use (NIST 800-175B)

Key Management:

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms. NIST 800-53 propose to use NIST FIPS-compliant or NSA-approved key management technology to produce, control and distribute symmetric cryptographic keys. In this study ISO/IEC 1170 and NIST 800-56A key management guidelines are used for key generation, control and distribution.

Source:

NIST 800-53 r5: SC-12

ISO IEC 27002 / ISO 27799: 10.1.2

NIST 800-56A

ISO/IEC 11770

Guidelines:

- Key management policy:
    - Maintain the availability of information in the event of the loss of cryptographic keys by users (SC-12)
    - A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle (SC-12, 10.1.2)
- Create key with appropriate key size and block size. Do not use a laptop or random application to generate the key. Only generate the key using any application or service provider which support hardware security modules (HSMs) (ISO/IEC 11770)
- Generated key needs to distribute securely so that it does not lose confidentiality and integrity (ISO/IEC 11770)
- Use key wrapping technique to exchange the key between mobile application and device. Diffie-Hellman key exchange provides the capability for two parties to agree upon a shared secret between them. It can be used for secret communication for exchanging cryptographic keys over a public channel (NIST 800-56A)
- If any user and/or device is identified as compromised, the respective key of user or device needs to remove from the application and key management server. After revocation of compromised key, a new key need to generate and distribute using above steps (ISO/IEC 11770)
- Logging each activity related to key management and use these data to perform auditing (10.1.2)

Non-Repudiation:

Implement proper countermeasure to protect against an individual cannot deny the action performed by them. Below is the list of countermeasures for non-repudiation while creating data, sending, receiving and approving any message.

Source:

NIST 800-53 r5: AU-10

ISO IEC 27002 / ISO 27799: 10.1.1

Guidelines:

- Bind identity of data generator such as user, sensor node device before sending any information (AU-10)
- Validate the data by sing cryptographic checksums to prevent data modification between generation and receiver end (AU-10)
- Use cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action (10.1.1)

Logging, Auditing and Accountability:

In WBAN application, it is necessary to keep track of each activity performed by an authorised and/or unauthorised user. Auditing is the process which will keep track of different types of event including password changes; failed log-on, key management, query parameters and file access. This audit record can be used generate evidence to make accountable a user for their action.

Source:

NIST 800-53 r5: AU-2, AU-3, AU-5, AU-6, AU-7, AU-8, AU-9, AU-5

ISO IEC 27002 / ISO 27799: 12.4.1, 12.4.2

Guidelines:

- Define the list of parameters will be captured as part of audit records and use a centralize platform to configure and manage these list of parameters (AU-3, 12.4.1)
    - user IDs
    - system activities
    - dates, times and details of key events, e.g. log-on and log-off
    - device identity or location if possible and system identifier
    - records of successful and rejected system access attempts
    - records of successful and rejected data and other resource access attempts
    - changes to system configuration
    - use of privileges
    - use of system utilities and applications
    - files accessed and the kind of access
    - network addresses and protocols
    - alarms raised by the access control system
    - activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems
    - records of transactions executed by users in applications.
- Limit the capturing of e-PHI and/or PHR data in audit records to minimise the privacy risk. If require anonymise the e-PHI and/or PHR data records before capturing in the audit log (AU-3, 12.4.1)

- Provide a warning to respective roles or owner within an organisation when allocated audit record storage volume reaches the maximum audit record storage capacity (AU-5, 12.4.2)
- Provide a real-time alert if the system failed to capture audit record in a time-period (AU-5)
- Implement an automated process to review and analysis the audit log which followed by generating report. Use this report to investigation and response to suspicious activities (AU-6)
- Implement the capability to sort and search audit records for an event based on the content fields of audit records (AU-7)
- Use internal system clocks to generate the timestamp fir audit records (AU-8)
- Implement cryptographic mechanisms to protect the integrity of audit records and assure only authorise user get access to these audit records. If require create an authorised user with read-only permission to audit record (AU-9)
- Initiate session audits including automatically file transfer, user request/response at the system start-up (AU-14)

Intrusion Detection:

Source:

NIST 800-53 r5: AU-13, SC-5, SC-7

ISO IEC 27002 / ISO 27799:

Guidelines:

- Implement automated mechanism to determine if any information disclosed in an unauthorised manner. Automated mechanism includes writing script or monitor new posts on selected website (AU-13)
- Denial of service may occur because of an attack by an adversary or a lack of internal planning to support organisational needs with respect to capacity and bandwidth. There are a variety of technologies available to limit or eliminate the effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by denial-of-service attacks (SC-5)
- Restrict the ability of individuals to launch denial of service attacks against other systems (SC-5)
- Employ monitoring tools to detect indicators of denial-of-service attacks against the system (SC-5)
- Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organisational security and privacy architecture. Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (SC-7)

- Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic (SC-7)
- Detect and deny outgoing communications traffic posing a threat to external systems and perform audit to identify the internal users associated with denied communications (SC-7)

Data integrity:

Source:

NIST 800-53 r5: SC-8, SI-7, SI-10

ISO IEC 27002 / ISO 27799:

Guidelines:

- Maintain the integrity of data during preparation for transmission and reception. Data can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing and unpacking (*SC-8)*
- Implement cryptographic mechanisms to prevent unauthorized disclosure of information or changes to information during transmission (*SC-8)*
- Perform an integrity check of software, firmware, and information at start up and provide notification upon discovering discrepancies during integrity verification (SI-7)
- Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information (SI-7)
- Verify the integrity of the boot process, assure only trusted code is executed during boot processes (SI-7)

- Implement cryptographic mechanisms to authenticate software or firmware components prior to installation (SI-7)

Data Input and Output Validation:

Source:

NIST 800-53 r5: SI-10

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- Check the validity of data inputs including; character set, length, numerical range, and acceptable values (SI-10)
- System need to handle invalid input data gracefully and return proper message to user (SI-10)
- Use regular expression to validate the whole string from an input and output dataset (OWASP)
- Assure that input validation is performed on both the client slide and server side (OWASP)
- Use standard data type validators available natively in web application frameworks or programming language use to develop the web and mobile application (OWASP)

Malware Protection:

Source:

NIST 800-53 r5:

ISO IEC 27002 / ISO 27799: 12.2.1

OWASP

Guidelines:

- Establishing a formal policy prohibiting the use of unauthorized software (*12.2.1*)
- Implementing controls that prevent or detect the use of unauthorized software (*12.2.1*)
- Implementing controls that prevent or detect the use of known or suspected malicious websites (*12.2.1)*
- Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated (*12.2.1)*
- Installation and regular update of malware detection and repair software in server to scan as a precautionary control, or on a routine basis; the scan carried out should include:
    - Scan any files received over networks or via any form of storage medium, for malware before use (*12.2.1)*
    - Scan web pages for malware (*12.2.1)*
- Implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware (*12.2.1)*

System Hardening:

Source:

NIST 800-53 r5: SR-9

ISO IEC 27002 / ISO 27799: 14.2.4

OWASP

Guidelines:

- Secure installation processes should be implemented, including (OWASP):
  - A repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to setup a new secure environment.
  - A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.
  - A task to review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process
- Implement a tamper protection program for the system, system component, or system service (SR-9)
- Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle (SR-9)
- Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled (14.2.4)

Incident Management Policy:

Source:

NIST 800-53 r5: IR-4, IR-5, IR-8

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- Implement an incident handling capability for incidents involving insider threats *(IR-4)*
- Establish and maintain an integrated incident response team that can be deployed to any time by the organisation *(IR-4)*
- Analyze malicious code and/or other residual artifacts remaining in the system after the incident *(IR-4)*
- Establish and maintain an integrated incident response team that can be deployed to any location identified by the organisation *(IR-4)*
- Automated mechanisms for tracking incidents and collecting and analyzing incident information include Computer Incident Response Centers or other electronic databases of incidents and network monitoring devices (IR-5)
- Include the following in the Incident Response Plan for breaches involving personally identifiable information: *(IR-8)*
  - A process to determine if notice to individuals or other organisations, including oversight organisations, is needed

  - An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms
  - Identification of applicable privacy requirements
- Develop an incident response plan that: *(IR-8)*
  - Provides the organisation with a roadmap for implementing its incident response capability
  - Describes the structure and organisation of the incident response capability
  - Provides a high-level approach for how the incident response capability fits into the overall organisation
  - Meets the unique requirements of the organisation, which relate to mission, size, structure, and functions
  - Provides metrics for measuring the incident response capability within the organisation
  - Addresses the sharing of incident information
  - Explicitly designates responsibility for incident response to organisation-defined entities, personnel, or roles
- Distribute copies of the incident response plan to organisation-defined incident response personnel (identified by name and/or by role)
- Update the incident response plan to address system and organisational changes or problems encountered during plan implementation, execution, or testing
- Protect the incident response plan from unauthorized disclosure and modification

Data Anonymisation:

Source:

NIST 800-53 r5: AC-3

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information (NIST 800-122)
- Implementing role-based access control and configuring it so that each user can access
- only the pieces of data necessary for the user‘s role (AC-3)
- Terms & Conditions (T&Cs) should be specifically for the use and data processing of the website (OWASP)
- Provide an easily readable summary of the terms and conditions as well as a long version (OWASP)
- Define the purpose of the collection of personal data.
- Only collect personal data required to fulfil the purpose
- Default is to collect as little data as possible unless the user chooses otherwise (data reduction / minimisation)

Backup Policy:

Source:

NIST 800-53 r5:

ISO IEC 27002 / ISO 27799: 12.3.1

OWASP

Guidelines:

- A backup policy should be established to define the organisation's requirements for backup of information, software and systems *(12.3.1)*
- Adequate backup facilities should be provided to assure that all essential information and software can be recovered following a disaster or media failure *(12.3.1)*
- Accurate and complete records of the backup copies and documented restoration procedures should be produced *(12.3.1)*
- The extent (e.g. full or differential backup) and frequency of backups (Hourly, Daily, Monthly) should reflect the business requirements of the organisation, the security and privacy requirements of the information involved and the criticality of the information to the continued operation of the organisation *(12.3.1)*
- The backups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site *(12.3.1)*
- Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site *(12.3.1)*
- In situations where confidentiality is of importance, backups should be protected by means of encryption *(12.3.1)*

Secure Software Update:

Source:

NIST 800-53 r5: SI-2

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it *(OWASP)*
- Apply integrity controls to files prior to transmitting them to sensor devices *(OWASP)*
- Add functionality for an automatic firmware update mechanism *(SI-2)*
- Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification *(OWASP)*
- Assure that the device software/firmware, its configuration and its applications have the ability to following capabilities:
  - update Over-The-Air (OTA)
  - update server is secure
  - update file is transmitted via a secure connection and does not contain sensitive data (e.g. hardcoded credentials)
  - update file is signed by an authorised trust entity and encrypted using accepted encryption methods
  - update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins

- Sign code cryptographically to assure it has not been tampered with after signing it as safe for the device, and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded *(OWASP)*
- Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful *(OWASP)*
- Keep all backend server updated and patched *(OWASP)*
- Notify user if they are not using the latest version of the firmware and/or mobile app

Device Management Policy:

Source:

NIST 800-53 r5:

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- Develop an end-of-life strategy for sensor device, mobile app and backend server
- Disclose the duration and end-of-life security and patch support (beyond product warranty)
- Monitor the performance and patch known vulnerabilities up until the “end-of-support" period of a product’s lifecycle
- Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections

- Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors
- Conduct periodic audits and reviews of controls to assure that the controls are effective. Perform penetration tests at least biannually
- Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage
- Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state
- Assure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems

System Monitoring:

Source:

NIST 800-53 r5: SI-4

ISO IEC 27002 / ISO 27799:

OWASP

Guidelines:

- Monitor the system to detect attacks and indicators of potential attacks
- Connect and configure individual intrusion detection tools into a system-wide intrusion detection system
- Employ automated tools and mechanisms to support near real-time analysis of events. Automated tools and mechanisms include host-based, network-based, transport-based,

or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis

- Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic. Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code
- Implement host-based monitoring mechanism
- Monitor inbound and outbound communications traffic
- Analyse communications traffic and event patterns for the system
- Develop profiles representing common traffic and event patterns
- Use the traffic and event profiles in tuning system-monitoring devices
- Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices
- Generate Alert when the following system-generated indications of compromise or potential compromise occur:
    - inputs from malicious code protection mechanisms
    - intrusion detection or prevention mechanisms
    - boundary protection devices such as firewalls, gateways, and routers
- Adjust the level of system monitoring activity when there is a change in risk to application or device operation
- Notify organisation-defined incident response personnel of detected suspicious events

Communication Security

Source:

NIST 800-53 r5: SC-8, SC-40

NIST SP 800-121 r2

OWASP

Guidelines:

- Implement strong, industry standard cryptographic mechanisms with appropriate key lengths to prevent unauthorized disclosure of information; detect changes to information] during transmission
- Implement strong, industry standard cryptographic mechanisms with appropriate key lengths to reduce the detection potential of wireless links which used for covert communications and to protect wireless transmitters from geo-location
- Implement strong, industry standard cryptographic mechanisms with appropriate key lengths that achieve against the effects of intentional electromagnetic interference
- Assume that the network layer is not secure and is susceptible to eavesdropping
- Apply SSL/TLS to transport channels that the mobile app will use to transmit sensitive information, session tokens, or other sensitive data to a backend API or web service.
- Never allow self-signed certificates, and consider certificate pinning for security conscious applications
- Always require SSL chain verification
- Only establish a secure connection after verifying the identity of the endpoint server using trusted certificates in the key chain
- Alert users through the UI if the mobile app detects an invalid certificate

- Choose PIN codes that are sufficiently random, long and private. Avoid static and weak PINs, such as all zeroes
- Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft
- The device must verify that an authenticated link key was generated during pairing
- Bluetooth devices should be configured by default as undiscoverable and remain undiscoverable except as needed for pairing
- Ensure device mutual authentication is performed for all connections
- Bluetooth devices must prompt the user to authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed
- Use application-level authentication and encryption atop the Bluetooth stack for sensitive data communication

Communication Security

Source:

OWASP

Blog Post

Guidelines:

- Use hardware-based Trusted Execution Environment (TEE) to assure data integrity, data confidentiality, and code integrity
- Implement proper access control so that an unauthorised entity cannot view or alter data in the Trusted Execution Environment
- Use Homomorphic Encryption (HE) and Trusted Platform Modules (TPM) to assure the protection of the data

- Provide a recoverability mechanism to recover a TEE from a non-compliant or potentially compromised state
- If the application is deployed in the cloud environment, then use cloud-provided confidential computing VM instances

Appendix D Case Study of a Fitness Tracking Application

This appendix shows how the data security and privacy risk management framework can be applied to the development of a WBAN application. Some of the stages presented have been implemented at a company and others were added after reflection on the implementation of a previous version of the framework at the company. This example does not consider the safety-related risk.

1 Initial Product Requirements

The purpose of this example is to illustrate how the framework can be applied to a WBAN application scenario, "FitnessX", a fitness tracking app. This product will use a physical activity monitoring device, which uses GPS and a series of sensors to track an athlete's activity during training and gameplay and relay this information to the app running on either iOS or Android over Bluetooth. In the app, users can sign up for an account and pair their device, before tracking sessions and syncing this data to the cloud. Session-based statistics and analysis can be used by the individual to track their performance and improvement and they can choose to share some of their data in a global leader-board. They can also create mini private or group leagues to use the same leader-board functionality among a closed group of individuals.

2 Security and Privacy Risk Assessment

The goal of conducting a security and privacy risk assessment is to identify, analyse and evaluate the potential security and privacy risk. As discussed in section 4.1 under Appendix B a security and privacy risk assessment will be conducted at the requirements analysis and system architecture phases by taking initial product requirements as input. The outcome of the security and privacy risk assessment stage will be a list of risks which will require security and privacy controls to mitigate.

2.1 Define scope and purpose

The overarching goals of the security and privacy risk assessment are to identify the risks to the security and privacy of the player's data. The primary objective includes assuring the confidentiality, integrity, availability and privacy of the data. Identification of the possible security and privacy risks of the application's features outlined in the previous section will be assessed. After that we need to identify and implement security controls to mitigate the security and privacy risks.

2.2 Risk Assessment Approach

Section 4.1.2 under Appendix B presented three different risk assessment approaches. This example assumes that the organisation will have limited knowledge and expertise to perform the security and privacy risk assessment. As the qualitative assessment approach is easy to perform and less time-consuming compared to the other two approaches, this approach will be selected for conducting the security and privacy risk assessment for the FitnessX application.

2.3 Risk assessment at the requirements analysis phase

The goal of conducting a risk assessment at the requirements analysis phase is to identify and evaluate the security and privacy risk. This assessment process will also help to identify the list of security and privacy requirements which need to be taken into consideration during the development of the system architecture. Below is the list of key tasks that will be conducted as part of a security and privacy risk assessment at the requirement analysis phase:

- Apply risk analysis to identify the security and privacy risks
- Evaluate each security and privacy risk to identify the acceptable and unacceptable risks
- Develop security and privacy requirements for unacceptable risks

The rest of the section is organised as follows; in section 2.3.1 identify the security and privacy risks by conducting risk analysis while section 2.3.2 outline the steps to evaluate the security and privacy risk and identify the list of unacceptable security and privacy risks which will require controls to mitigate. Finally, section 2.3.3 outlines the list of security and privacy requirements.

2.3.1 Security and privacy Risk analysis

The goal of the security and privacy risk analysis step is to identify the security and privacy risk. As part of the security and privacy risk analysis, the following four tasks need to be conducted.

- **Identify and document the assets**

Assets of FitnessX application include sensor devices, information collected by the sensor devices, and server instances which are used to process and store the data. Asset identification also should include those assets needed by the user to manage user information, fitness-related data, and components of the device including the device software. Figure Appendix D-1 illustrated the list of assets for the FitnessX application.

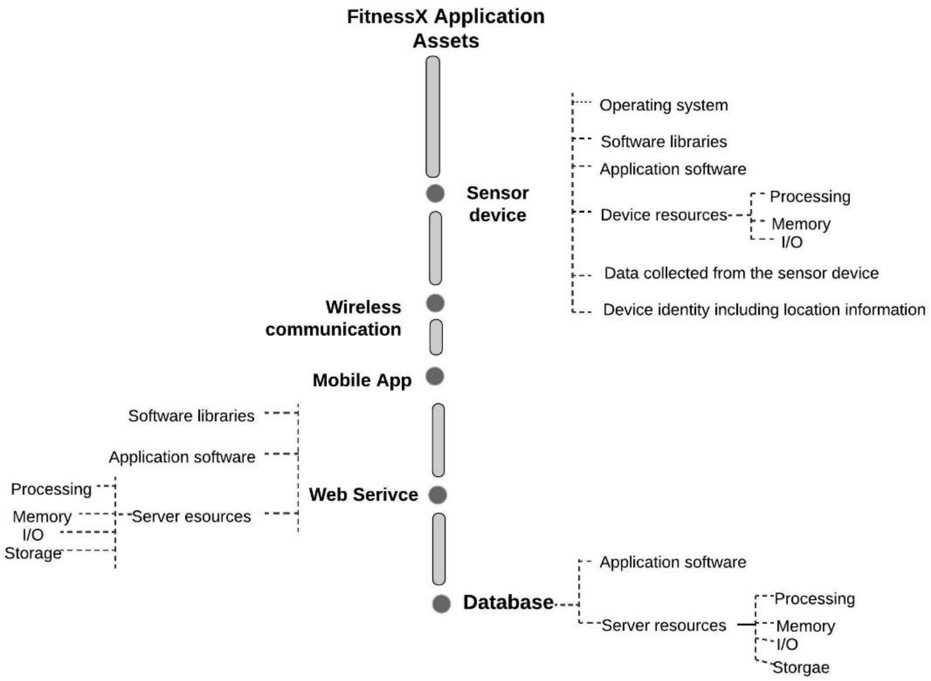


Figure Appendix D-1: List of assets for FitnessX system

- **Identify and document the threats**

The goal of this stage is to identify the possible threats to the FitnessX application at the requirement analysis phase. As discussed in section 4.1.3.1 under Appendix B threats will be identified based on the assets from the previous stage. Table Appendix E-1 under Appendix E will be utilised to identify the threats with respect to each asset. Table Appendix D- 1 presents a list of threats for the FitnessX application.

Table Appendix D- 1: Sample list of threats for the FitnessX application

Asset Name	Threats
Sensor Device	Communication protocol hijacking
	Code Injection
	Manipulation of Hardware or Software
	Repudiation Attack
	Replay attack
	Modification of information
Mobile App	Cross Site Scripting (XSS)
	Cryptanalysis
	Custom Special Character Injection
	Man-in-the-middle attack
	Physical attacks
	HTTP Response Splitting
Wireless communication	Eavesdropping
	Masquerading attack
	Man-in-the-middle attack
	Modification of information
	Sniffing attack
Web Service	Repudiation Attack

Asset Name	Threats
	SQL Injection
	Replay attack
	Denial of Service
Database	Denial of Service
	Sensitive information leakage
	Loss of devices, storage media and documents
	Information from an unreliable source
	Physical attacks

- **Identify and document the vulnerabilities**

The possible vulnerabilities at the requirements phase will be select from Table Appendix E-1 under Appendix E based on the assets and threats identified in the previous stage. Table Appendix D- 2 presents a sample list of vulnerabilities for the FitnessX application.

Table Appendix D- 2: Sample list of vulnerabilities for the FitnessX application

Asset Name	Threats	Vulnerabilities
Sensor Device	Communication protocol hijacking	Insecure Communication
	Code Injection	Input Validation Vulnerability
	Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings
	Repudiation Attack	Access Control Vulnerability Logging and Auditing Vulnerability
	Replay attack	Lack of session management Insufficient Cryptography
	Modification of information	Insecure Communication Insecure Data Storage
Mobile App	Cross Site Scripting (XSS)	Improper Data Validation
	Cryptanalysis	Insufficient Cryptography
	Custom Special Character Injection	Input Validation Vulnerability
	Man-in-the-middle attack	Session Management Vulnerability Insecure Communication
	Malware	Security defects in the software Insecure design or user error Over-privileged users Over-privileged code Use of the same operating system
	HTTP Response Splitting	Input validation vulnerability
Wireless communication	Eavesdropping	Insecure communication
	Masquerading attack	Lack of access Control Insecure Authorization Insufficient Cryptography
	Man-in-the-middle attack	Session management vulnerability insecure communication
	Modification of information	Insecure communication
	Sniffing attack	Insecure communication
Web Service	Repudiation Attack	Access control vulnerability Logging and auditing vulnerability
	SQL Injection	Input validation vulnerability
	Replay attack	Lack of session management Insufficient cryptography
	Denial of Service	Input validation vulnerability API abuse Lack of intrusion detection
	Man-in-the-middle attack	Session management vulnerability insecure communication

Asset Name	Threats	Vulnerabilities
	Manipulation of hardware or software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings
Database	Denial of Service	Input validation vulnerability Lack of intrusion detection Database access abuse
	Sensitive information leakage	Insecure data storage Insecure communication
	Loss of devices, storage media and documents	Lack of device management Lack of auditing Lack of backup policy
	Information from an unreliable source	Lack of access control Insecure authorisation
	Buffer overflow attack	Buffer overflow
	Physical attack	Lack of physical hardening

2.3.2 Risk evaluation and treatment

The risk evaluation process helps organisations to determine whether the identified risks are acceptable or not. The result of the multiplication of impact and likelihood level of the identified risk will help to identify the risk acceptability. First, the organisation needs to set the threshold of the risk acceptability level. In this example scenario, the risks with a low or very low score set as the threshold level for acceptable risks. So, risk acceptability score will be four, as the multiplication of impact and likelihood (Low (2) x Low (2)) is equal to four. If any risk's acceptability score is less than or equal to four it will not be taken into consideration for future analysis. Table Appendix D- 3 illustrates the security risk evaluation of the threats and vulnerabilities identified in Table Appendix D- 2.

Table Appendix D- 3: Risk evaluation in the requirements analysis phase

Security and privacy risks	Likelihood of Occurrence	Impact	Risk Score (Impact * Likelihood)	Risk Acceptability
Insecure Communication	Very High	Very High	Very High (Score=25)	Unacceptable
Input Validation Vulnerability	Very High	Very High	Very High (Score=25)	Unacceptable
Manipulation of Hardware or Software	Medium	Medium	Medium (Score=9)	Unacceptable
Repudiation Attack	Very High	Very High	Very High (Score=25)	Unacceptable
Replay attack	High	High	High (Score=16)	Unacceptable
Access Control Vulnerability	High	High	High (Score=16)	Unacceptable
Insufficient Cryptography	Very High	Very High	Very High (Score=25)	Unacceptable
Man-in-the-middle attack	Very High	Very High	Very High (Score=25)	Unacceptable
Insecure Data Storage	Very High	Very High	Very High (Score=25)	Unacceptable
Malware attack on mobile app	Medium	Medium	Medium (Score=9)	Unacceptable
Hard-coded or factory default passcodes	High	High	High (Score=16)	Unacceptable
Manipulation of hardware or software of web service	Very Low	High	Low (Score=)	Acceptable
Buffer overflow attack on database	Very Low	High	Low (Score=4)	Acceptable

As the database is only accessible from web service, so the likelihood of lunching a buffer overflow attack on a database is Very Low. Although the impact of this attack is High, the total risk score is equal to four (Very Low (1) x High (4) = 4). So, the "Buffer overflow attack on database" is an acceptable risk. Upon identifying the unacceptable risks for the FitnessX application, the next task is to identify which of them will require security and privacy controls to mitigate. Table Appendix D- 4 presents the risk treatment for unacceptable security and privacy risks identified in Table Appendix D- 3.

Table Appendix D- 4: Risk treatment for unacceptable risks

Security and privacy risks	Risk Acceptability	Risk Treatment
Insecure Communication	Unacceptable	Require security control
Input Validation Vulnerability	Unacceptable	Require security control
Manipulation of Hardware or Software	Unacceptable	Require security control
Repudiation Attack	Unacceptable	Require security control
Replay attack	Unacceptable	Require security control
Access Control Vulnerability	Unacceptable	Require security control
Insufficient Cryptography	Unacceptable	Require security control
Man-in-the-middle attack	Unacceptable	Require security control
Insecure Data Storage	Unacceptable	Require security control
Malware attack on the mobile app	Unacceptable	Risk share with the end-user
Hard-coded or factory default passcodes	Unacceptable	Require security control

As the app will be installed on the mobile device managed by the user, it will have limited access to implement any control to mitigate attacks like *"Malware attack on the mobile app"*. So, this risk will be shared with the end-user by providing some best practice guidelines to prevent malware attacks.

2.3.3 Updated security and privacy requirements

The goal of this stage is to update the security and privacy requirements from the list of unacceptable security and privacy risks identified at the previous stage, which require control to mitigate. The proposed security and privacy risk control in Table Appendix E-1 under Appendix E for the respective unacceptable security risk is taken into consideration during the development of security and privacy requirement. Below is the list of security and privacy requirements for the FitnessX application:

- Implement proper authentication and authorisation process to check the identity of the user before allowing access to the data
- Use a lightweight, memory and energy-efficient cryptographic algorithm for encryption support in the sensor device
- Always transmit encrypted data over Bluetooth from the sensor device to the mobile app
- Use a key management service for key generation, key refreshing, key agreement, key distribution and key revocation
- Use only HTTPS communication between the mobile app and the backend server
- Encrypt all data before storing in the sensor device and database
- Include proper logging techniques for auditing and accountability
- Include data backup strategy to assure high availability of the application

2.4 Security and privacy risk assessment at the system architecture phase

The objective of conducting a security and privacy risk assessment at the system architecture phase is similar to the requirement analysis phase. Below are the key tasks that need to be conducted at this phase as part of security and privacy risk assessment:

- Review system architecture according to security principles and, security and privacy requirements
- Apply risk analysis to identify the security and privacy risk
- Evaluate each security and privacy risk to identify the acceptable and unacceptable risks

- Identify the list of unacceptable risks which will require controls to mitigate using risk treatment

2.4.1 Review system architecture

The goal of this stage is to review the system architecture for the FitnessX application Figure Appendix D-2 illustrated the system architecture of the FitnessX application, which was reviewed based on the guidelines outline in section 4.1.4.1 under Appendix B. The outcome of the review process was no further changes required on the current system architecture.

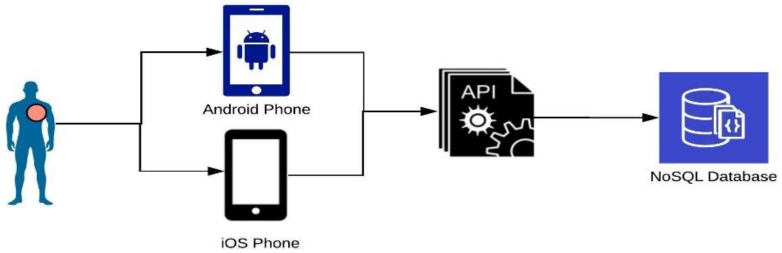


Figure Appendix D-2: The system architecture of the FitnessX application

2.4.2 Risk analysis

The goal of this stage is to conduct a risk analysis to identify the assets, threats and vulnerabilities based on the system architecture. Risk analysis will be conducted using a similar process to that used during the requirements analysis phase.

- **Identify and document the assets**

As no additional assets were introduced at the system architecture phase the same list of assets from the requirement phase, which is presented in Figure Appendix D-1 will be reused at this phase.

- **Identify and document the threats**

As no additional asset were introduced at the system architecture phase, he same list of threats from the requirements phase will be reused in this phase.

- **Identify and document the vulnerabilities**

A threat modelling or attack tree technique can be used to identify the vulnerabilities in the system architecture phase. The rest of this section demonstrates how to conduct threat modelling and use attack trees to identify the vulnerabilities of the FitnessX application.

Threat Modelling

Threat modelling is a widely recognised process for identifying possible threats to an application and is considered a significant step in assuring security. Threat modelling also helps to establish a solid basis to specify and prioritise the security and privacy requirements to implement proper countermeasures.

STRIDE is a widely recognised threat modelling technique for web-based applications. It was developed by Microsoft, which also provide an open-source tool named the Microsoft Threat Modelling Tool (TMT). This tool includes a graphical interface to conduct threat modelling. By using the graphical interface, a user can easily design the data flow diagram, configure necessary parameters and track the threat with respective implementation status. Conducting threat modelling using this tool is done in three steps:

1) Design and configuration
2) Generate threat report
3) Identify the security controls by analysing the report

The design and configuration step starts by drawing the Data Flow Diagram (DFD) using the Microsoft TMT. This DFD diagram is enhanced by adding the proper data flows, data stores, processes, interactors, and trust boundaries. Each of the DFD element properties is configured based on respective element behaviour. For example, device attribute properties are configured by setting “Yes” to GPS, data, store log data, encrypted, write access, removable storage and backup. After that, each of the DFD elements is connected by defining the proper connectivity attribute.

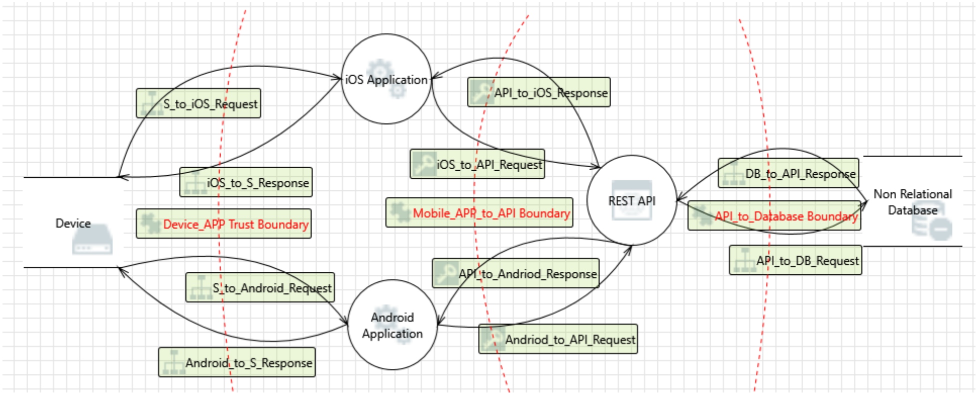


Figure Appendix D-3: DFD diagram in Microsoft Threat modelling Tool

The connectivity attribute is set to “Bluetooth” from device to iOS and Android mobile app, and mobile app to REST API is set to “Wi-Fi”. The REST API to Non-Relational database is configured as “wired” as both are deployed in cloud infrastructure. Finally, a trust boundary is configured to enable the trust level between DFD elements for data exchange. Figure Appendix D-3 illustrates the updated DFD of the application in the Microsoft TMT tool.

One of the key features of the Microsoft TMT tool is the ability to generate a threat report based on the DFD and element attributes. The threat report consists of a list of threats, threat categories, data flow directions and respective descriptions. The description of each threat will help to identify the proper security control for countermeasures. After exporting the threat report from the TMT tool, each threat needs to be reviewed to identify appropriate security controls. During the review process, each threat description, threat type and data flow interaction needs to be considered. In some cases, if a threat does not contain enough description of the threat, then the threat category will be used to select a security control as a countermeasure. Table Appendix D- 5 illustrates some sample threats and vulnerabilities with respective details which are identified using Microsoft TMT tool.

Table Appendix D- 5: Sample vulnerabilities identified using Microsoft TMT tool

vulnerabilities	Description
Weak Credential Transit	Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in

vulnerabilities	Description
	the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.
The Device Data Store Could Be Corrupted	Data flowing across iOS_to_S_Response may be tampered with by an attacker. This may lead to corruption of Device. Assure the integrity of the data flow to the data store.
Potential Weak Protections for Audit Data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs or attack log analysis programs. Assure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect
Risks from Logging	Log readers can come under attack via log files. Consider ways to canonicalise data in all logs. Implement a single reader for the logs, if possible, to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.
Potential Process Crash or Stop for REST API due to the DDOS attack	Attacker lunch DDOS attack, which will result in REST API crashes, halts, stops or runs slowly and make the application unavailable.
Replay Attacks	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilise an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.
Potential Data Repudiation by REST API	REST API claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Weak Authentication Scheme	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.
Potential Lack of Input Validation for REST API	Data flowing across Android_to_API_Request may be tampered with by an attacker. This may lead to a denial of service attack against REST API or an elevation of privilege attack against REST API or an information disclosure by REST API. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Attack Trees

Attack trees attempt to model all possible threats against an application and to identify all of the possible ways in which the application can be attacked. A tree structure is used to represent the attacks against an application, with the goal as the root node and different ways of achieving that goal as leaf nodes. Below is the list of steps to conduct attack tree analysis:

- Define the attacker overall goal; such as disrupt the application service, privacy attack
- Decompose the overall goal into sub goals; such as compromise application availability , data tampering or identity privacy leakage
- Continue stepwise decomposition into smaller task and assign to leaf nodes
- Use “OR” nodes to represent alternatives and “AND” nodes to represent all different steps for achieving the goal

There are various tools available such as ADTool, Ent, SeaMonster for modelling attack trees of an application. In this framework the ADTool is use for modelling the attack tree. Figure Appendix D-4 represents the FitnessX application disruption attack tree model.

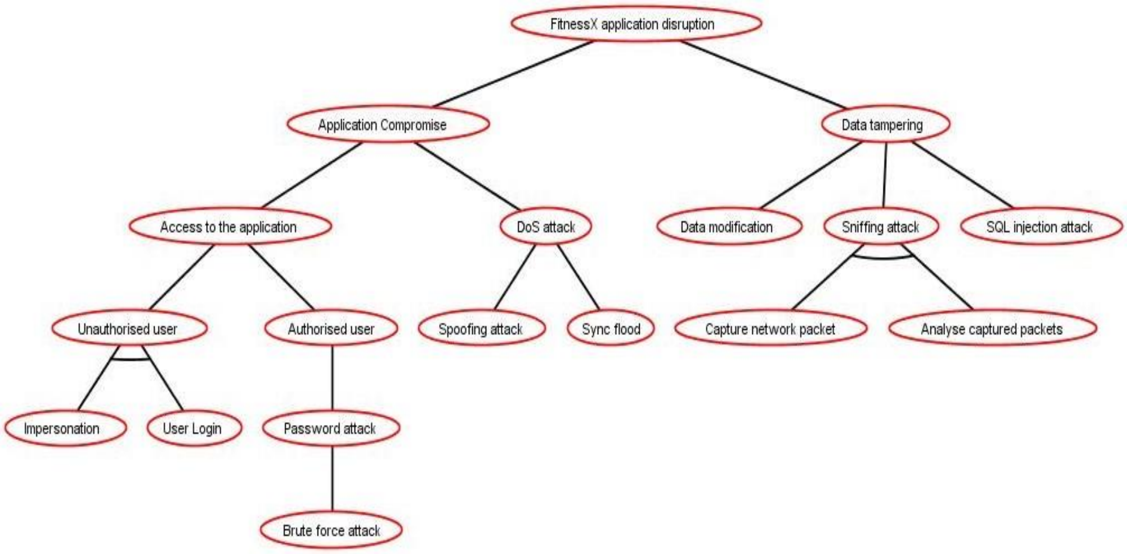


Figure Appendix D-4: FitnessX application disrutpion attack tree model

2.4.3 Risk evaluation and treatment

The goal of this section is to evaluate security and privacy risks to identify the acceptable and unacceptable risk. To evaluate the security and privacy risk, a similar process will be followed as outlined in the previous section 2.3.1 under Appendix D. Table Appendix D- 6 presents the list of security and privacy risks with a calculated risk score and risk acceptability.

Table Appendix D- 6: Risk evaluation in the system architecture phase

Security and privacy risks	Likelihood of Occurrence	Impact	Risk Score (Impact * Likelihood)	Risk Acceptability
Weak authentication scheme	Very High	Very High	Very High (Score=25)	Unacceptable
Weak credential transit	Very High	Very High	Very High (Score=25)	Unacceptable
Potential Data Repudiation by Android and/or ios Application	Medium	Medium	Medium (Score=9)	Unacceptable
Potential process crash or stop for REST API due to the DDOS attack	Very High	Very High	Very High (Score=25)	Unacceptable
Potential weak protections for audit data	High	High	High (Score=16)	Unacceptable
Lack of data input validation	Very High	Very High	Very High (Score=25)	Unacceptable
Lack of encryption on transmitted data	Very High	Very High	Very High (Score=25)	Unacceptable
Lack of encryption on private/sensitive data at rest	Very High	Very High	Very High (Score=25)	Unacceptable
Lack of physical tamper detection and response	Medium	Medium	Medium (Score=9)	Unacceptable
Weak remote access controls	Medium	Medium	Medium (Score=9)	Unacceptable
Lack of system hardening	High	High	High (Score=16)	Unacceptable

Security and privacy risks	Likelihood of Occurrence	Impact	Risk Score (Impact * Likelihood)	Risk Acceptability
Potential process crash or stop for iOS / Android application	Low	Low	Low (Score=4)	Acceptable
iOS / Android application process memory tampered	Low	Low	Low (Score=4)	Acceptable

Upon identifying the unacceptable risks for the FitnessX application, the next task is to identify which of them will require security and privacy control to mitigate. Table Appendix D- 7 presents the risk treatment for unacceptable security and privacy risks identified in Table Appendix D- 6.

Table Appendix D- 7: Risk treatment for unacceptable risks

Security and privacy risks	Risk Acceptability	Risk Treatment
Weak Authentication Scheme	Unacceptable	Require security control
Weak Credential Transit	Unacceptable	Require security control
Potential Data Repudiation by Android and/or iOS Application	Unacceptable	Require security control
Potential Process Crash or Stop for REST API due to the DDOS attack	Unacceptable	Require security control
Potential Weak Protections for Audit Data	Unacceptable	Require security control
Lack of data input validation	Unacceptable	Require security control
Lack of encryption on transmitted data	Unacceptable	Require security control
Lack of encryption on private/sensitive data at rest	Unacceptable	Require security control
Lack of physical tamper detection and response	Unacceptable	Require security control
Weak remote access controls	Unacceptable	Require security control
Lack of system hardening	Unacceptable	Require security control

3 Security and Privacy Risk Control

Security and privacy risk controls are the safeguards or countermeasures to mitigate the threats and vulnerabilities of the application. The goal of this section is to identify the countermeasures for unacceptable security and privacy risks identified in the previous section, followed by examples of the implementation of the selected security and privacy controls.

3.1 Selection of security and privacy risk controls

The goal of this stage is to identify the security and privacy controls for the list of unacceptable risks identified during the security and privacy risk assessment at both the requirements analysis and the system architecture phase. Identification of security and privacy controls will be conducted by taking the following two key items into consideration:

- Get the respective security and privacy control from Table Appendix E-1 under Appendix E for each unacceptable security and privacy risk from the requirement analysis phase which requires controls to mitigate
- Get the security and privacy controls for each unacceptable risk from the system architecture phase which requires controls to mitigate by analysing the recommendation provided by the threat modelling tool

Table Appendix D- 8 outlines the security controls for some of the unaccepted security and privacy risk which requires control to mitigate

Table Appendix D- 8: Controls for respective security and privacy risk

Security and privacy risk	Control
Weak Authentication Scheme	Authentication
Weak Credential Transit	Authentication, Encryption
Potential Data Repudiation by Android and/or iOS Application	Auditing, Non-repudiation
Potential Process Crash or Stop for REST API due to the DDOS attack	Access Control, Intrusion Detection, Auditing
Lack of data input validation	Data Integrity, Input validation
Lack of encryption on transmitted data	Encryption, Communication security
Lack of encryption on private/sensitive data at rest	Encryption
Lack of physical tamper detection and response	Physical Protection
Weak remote access controls	Access Control
Lack of system hardening	Physical Protection, Client Platform security

3.2 Implementation of the security and privacy control

Upon completion of the security and privacy risk control selection process, the next task is to implement the selected security and privacy risk controls. The developer needs to follow the implementation details outlined in Appendix C for each selected security and privacy risk control. The examples below illustrate the implementation details for two security and privacy risks from Table Appendix D- 8.

Security and privacy risk name: *Weak Authentication Scheme*

Control: *Authentication*

Implementation details: *An authentication scheme needs to be implemented. To develop an authentication scheme, guidelines outlined in Appendix C under the Authentication section need to be taken into consideration. The developer needs to implement an authentication scheme which will:*

- *Force users to have a strong password*
- *Not display or transmit the password in clear text. Validate the email address and password through an input validation technique*
- *Validate email address by sending the email verification link*
- *Lock user accounts after a certain number of failed logins attempts during a time-period*
- *Maintain a list for commonly used, expected, or compromised passwords and update the list when passwords are compromised directly or indirectly*

Security and privacy risk name: *Potential Data Repudiation by Android and/or iOS Application*

Control: *Auditing, Non-repudiation*

Implementation details: T*wo security controls Auditing and Non-repudiation need to be implemented. To identify the source of data, each of the requests coming to the REST API needs to be captured. As outlined in Appendix C under the Auditing section, the developer needs to capture the list of parameters with each request. The captured log with the list of parameters will be useful during the auditing process to identify the source of the data.*

- *Bind identity of data generator such as user, sensor node device before sending any information*
- *Validate the data by using cryptographic checksums to prevent data modification between generation and receiver end*
- *Use cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action*
- *Define the list of parameters which will be captured as part of audit records and use a centralise platform to configure and manage this list of parameters*
  - *User ids*
  - *System activities*
  - *Dates, times and details of key events, e.g. Log-on and log-off*
  - *Device identity or location if possible and system identifier*
  - *Records of successful and rejected data and other resource access attempts*
  - *Network addresses and protocols*
  - *Records of transactions executed by users in applications*

3.3 Unit Testing

Unit testing is a testing method which helps to test an individual unit or component of an application. The goal of unit testing for this example will be to validate that each control is implemented as designed. The example below details the test to validate that the countermeasure for "*Weak Authentication Scheme*" is properly implemented.

Sample use case: *User login with username and password*

Test objectives: *Verify that the identity requirements for user authentication are aligned with business and security and privacy requirements*

Acceptance criteria:

ID	Test case	Expected result
TEST01	Testing for Valid user/right password	Successful authentication response
TEST02	Testing for valid user/wrong password	Authentication failed due to the wrong password
TEST03	Testing for a nonexistent username	Authentication failed due to invalid username
TEST04	Testing authentication with blank passwords	Authentication failed due to empty password supplied
TEST05	Attempt to log in with an incorrect password four times	Account locked out due to maximum try with the wrong password. Please contact the administrator.

4 Evaluation of overall residual security and privacy risk acceptability

The goal of this stage is to evaluate the efficacy of the controls implemented to mitigate the threats and vulnerabilities. As discussed in section 4.3 under Appendix B, penetration testing and/or vulnerability scanning can be used to assess the overall residual security and privacy risk of an application. So, a penetration test was conducted with the help of a third-party penetration service provider. The rest of the section is organised as follow; section 4.1 outline the scope of the testing followed by testing methodology in section 4.2. Section 4.3 outline the list of tools used to conduct the testing. Finally, section 4.4 present the test results with the recommendation to mitigate the identified vulnerabilities.

4.1 Scope of the testing

Penetration testing seeks to evaluate the security risk control implemented as a countermeasure for threats and vulnerabilities by using simulated attacks to identify and exploit the threats and vulnerabilities. Before conducting the penetration test, one of the most critical tasks is to define the scope of the testing. Usually, the scope consists of what networks, applications, databases, accounts, people, physical security controls and assets will be attacked during the testing. In this example, only “Web Service” and “No-SQL database” of the application will be considered for conducting penetration testing. Testing will be performed using industry-standard penetration tools and frameworks.

4.2 Testing Methodology

Penetration testing can be done with a combination of manual and automated methods. The tools and methods used for exploitation during penetration testing are intended to compromise systems with malicious intent. Before testing starts, clear ground rules need to be established to assure the stop points. This helps to assure that unexpected damage to systems does not occur. For instance, when testing a web server which contains an SQL injection flaw, it is enough to identify the compromise without attempting to obtain further access to the database servers. Network requests are relayed through several tools for manual and automated inspection, to allow listening and watching what the platform was doing. These data dumps are then taken into different tools and tested for any sort of injection points, as well as further manual investigation.

4.3 Testing Tools

As discussed in the previous section penetration testing can be conducted using a combination of manual and automated tools. Table Appendix D- 9 illustrates some of the automated tools uses during penetration testing.

Table Appendix D- 9: List of automated tools for penetration testing

Name	Description
Apache ab test	Apache ab load test tool uses to generate the number of request per second. This tool very useful to perform load testing and DDOS attack scenario.
OWASP ZAP	The Open Web Application Security Project - Zed Attack Proxy (ZAP) is a penetration testing tool for finding vulnerabilities in applications.
BURP SUITE	Burp Suite is a platform for performing security testing of applications.
NMAP	Nmap (Network Mapper) is a free and open-source utility for network exploration or security auditing.
SSLSCAN	SSLScan tests for different SSL exploits, such as heartbleed and the POODLE vulnerability, it also tests the cipher suites and key exchanges.
HYDRA brute force	Hydra is a rapid dictionary attacker which can be configured against over 50 different protocols. It is most commonly used for brute-forcing user accounts to test for weak passwords.
KALI LINUX	Kali is a Debian-derived Linux distribution designed for digital forensics and penetration testing installed with hundreds of different tools.

4.4 Penetration Test Result

There were two different types of vulnerabilities identified by penetration testing. The penetration service provider also includes the recommendation along with test result to mitigate the identified vulnerabilities. Below is the list of vulnerabilities along with recommendation which were identified during the penetration testing:

- **Potential denial of service points:** During testing, there were four potential DDoS points found. These are requests that timeout within 10s due to malformed data inside the payload. These can be run multiple times in multiple threads, driving up the usage and putting stress and strain on the service.

  Recommendation: It was advised that the API endpoints backend code should handle potential malformed data gracefully by assessing each field from the payload. Additionally, a proper HTTP response need to add if API endpoint failed to process, so that the user can retry a request later.

  Action: Added input validation to validate the input data stream. Additionally, an error response code also added to notify user that API endpoints were unable to process the malformed input data

- **Security misconfiguration – Stack traces enabled**: During testing, it was discovered that stack traces were enabled for some API endpoints.

  Recommendation: It was advised to tun off the stack trace for all endpoints and use a code review process to detect this codding error during the development.

  Action: Stack trace was disable for all the endpoints and the exception was written into a log file for auditing. Additionally, code review process was also added as a step in the framework.

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

A non-exhaustive list of assets, possible threats, vulnerabilities, and respective controls for WBAN applications is presented in Table Appendix E-1.

Table Appendix E-1: List of Assets, Threats, Vulnerability, and Respective Controls for WBAN Application

Asset Name	Asset Sub-category	Threat Name	Vulnerabilities	Security Controls
Sensor Device	**Operating system**	Malware	Over-privileged users Over-privileged code	**Malware Protection**
		communication protocol hijacking	Insecure Communication	**Cryptography and Encryption** **Authentication and Authorisation**
		Code Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	**System Hardening** **Logging, Auditing and Accountability** **Secure Software Update**
		Failure of system	Lack of System Monitoring	**System Monitoring** **Malware Protection** **Incident Management Policy**
	Software libraries	Malware	Security defects in software Insecure design or user error Over-privileged code	**Malware Protection**
		Injection attack	Input Validation Vulnerability	**Data Input and Output Validation**
		Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	**Logging, Auditing and Accountability** **Secure Software Update** **System Hardening**
	Application software	Malware	Security defects in software Insecure design or user error Over-privileged code	**Malware Protection**
		Code Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Cryptanalysis	Insufficient Cryptography	**Cryptography and Encryption** **Key Management**
		Log Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Repudiation Attack	Access Control Vulnerability Logging and Auditing Vulnerability	**Logging, Auditing and Accountability** **Access Control** **Non-Repudiation**
		Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	**System Hardening** **Logging, Auditing and Accountability** **Secure Software Update**
	Device identity including location information	Malware	Security defects in software Insecure design or user error Over-privileged users Over-privileged code	**Malware Protection**

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

Asset Name	Asset Sub-category		Threat Name	Vulnerabilities	Security Controls
			Attacks on privacy	Insecure Data Storage Insufficient Privacy Protection	**Cryptography and Encryption** **Authentication and Authorisation** **Data Anonymisation**
			Modification of information	Insecure Communication Insecure Data Storage	**Cryptography and Encryption** **Data integrity**
			Data / Sensitive information leakage	Insecure Data Storage	**Cryptography and Encryption** **Authentication and Authorisation** **Data Anonymisation**
			Replay attack	Lack of session management Insufficient Cryptography	**Authentication and Authorisation** **Cryptography and Encryption**
	Data collected from the sensor device		Malware	Security defects in software Over-privileged users Over-privileged code	**Malware Protection**
			Attacks on privacy	Insecure Data Storage Insufficient Privacy Protection	**Cryptography and Encryption** **Authentication and Authorisation** **Data Anonymisation**
			Modification of information	Insecure Communication Insecure Data Storage	**Cryptography and Encryption** **Data integrity**
			Data / Sensitive information leakage	Insecure Data Storage	**Cryptography and Encryption** **Authentication and Authorisation** **Data Anonymisation**
			Replay attack	Lack of session management Insufficient Cryptography	**Authentication and Authorisation** **Cryptography and Encryption**
	Device resources	**Processing**	Malware	Security defects in software Insecure design or user error Over-privileged code	**Malware Protection**
			Buffer Overflow Attack	Buffer Overflow	**Code Review**
		Memory	Malware	Security defects in software Insecure design	**Malware Protection**
			Buffer Overflow Attack	Buffer Overflow	**Code Review**
		I/O	Malware	Security defects in software Insecure design	**Malware Protection**
			Communication protocol hijacking	Insecure Communication	**Cryptography and Encryption** **Authentication and Authorisation**
			Masquerading attack	Lack of Access Control Insecure Authorization Insufficient Cryptography	**Access Control** **Authentication and Authorisation** **Cryptography and Encryption**
			Network reconnaissance	Insecure communication Lack of System Hardening	**Cryptography and Encryption** **System Hardening**
			Side channel attack	Insecure communication	**Cryptography and Encryption**
			Denial of Service	Input Validation Vulnerability Lack of intrusion detection	**Data Input and Output Validation** **Intrusion Detection** **System Monitoring**
			Physical attacks	Lack of Physical Hardening	**Physical Protection** **Client Platform Security**
			Theft of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing	**Device Management Policy** **Logging, Auditing and Accountability**
			Loss of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing	**Device Management Policy** **Logging, Auditing and Accountability**
			Natural Disaster	Lack of physical protection	**Physical Protection**

Asset Name	Asset Sub-category	Threat Name	Vulnerabilities	Security Controls
		Failures of devices	Lack of Device Monitoring	**System Monitoring** **Malware Protection** **Incident Management Policy**
Mobile App		Malware	Security defects in software Insecure design or user error Over-privileged users Over-privileged code	**Malware Protection**
		Buffer Overflow Attack	Buffer Overflow	**Code Review**
		Code Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Cross Site Scripting (XSS)	Improper Data Validation	**Data Input and Output Validation**
		Cryptanalysiss	Insufficient Cryptography	**Cryptography and Encryption** **Key Management**
		Custom Special Character Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Function Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Man-in-the-middle attack	Session Management Vulnerability Insecure Communication	**Authentication and Authorisation** **Data Input and Output Validation** **Cryptography and Encryption**
		Mobile code invoking untrusted mobile code	Unsafe Mobile Code	**Static Code Analysis** **Code Review**
		Mobile code non-final public field	Unsafe Mobile Code	**Access Control**
		Mobile code object hijack	Input Validation Vulnerability	**Data Input and Output Validation**
		Setting Manipulation	General Logic Error Vulnerability	**Code Review** **Secure Coding guideline**
		Special Element Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Unicode Encoding	Input Validation Vulnerability	**Data Input and Output Validation**
		Web Parameter Tampering	Input Validation Vulnerability	**Data Input and Output Validation**
		Physical attacks	Lack of Physical Hardening	**Physical Protection** **Client Platform Security**
		Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	**System Hardening** **Logging, Auditing and Accountability** **Secure Software Update**
		Theft of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing	**Device Management Policy** **Logging, Auditing and Accountability**
		Loss of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing	**Device Management Policy** **Logging, Auditing and Accountability**
		HTTP Response Splitting	Input Validation Vulnerability	**Data Input and Output Validation**
		Session Prediction	Input Validation Vulnerability	**Data Input and Output Validation**
		Session fixation	Session Management Vulnerability	**Authentication and Authorisation**
		Session hijacking attack	Input Validation Vulnerability	**Authentication and Authorisation**
		Failure of system	Lack of System Monitoring	**System Monitoring** **Malware Protection** **Incident Management Policy**

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

Asset Name	Asset Sub-category	Threat Name	Vulnerabilities	Security Controls
		Information or Products from an Unreliable Source	Lack of Access Control Insecure Authorisation	**Access Control** **Authentication and Authorisation**
Web Application		Malware	Security defects in software Insecure design or user error Over-privileged users Over-privileged code	**Malware Protection**
		Buffer Overflow Attack	Buffer Overflow	**Code Review**
		Code Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Cross Site Scripting (XSS)	Improper Data Validation	**Data Input and Output Validation**
		Cryptanalysiss	Insufficient Cryptography	**Cryptography and Encryption** **Key Management**
		Custom Special Character Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Execution After Redirect (EAR)		**Access Control**
		Function Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Man-in-the-middle attack	Session Management Vulnerability Insecure Communication	**Data Input and Output Validation** **Authentication and Authorisation** **Cryptography and Encryption**
		Mobile code object hijack	Input Validation Vulnerability	**Data Input and Output Validation**
		Special Element Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Web Parameter Tampering	Input Validation Vulnerability	**Data Input and Output Validation**
		Form action hijacking	Input Validation Vulnerability	**Data Input and Output Validation**
		Session Prediction	Input Validation Vulnerability	**Data Input and Output Validation**
		Session fixation	Session Management Vulnerability	**Authentication and Authorisation**
		Session hijacking attack	Input Validation Vulnerability	**Authentication and Authorisation**
		Failure of system	Lack of System Monitoring	**System Monitoring** **Malware Protection** **Incident Management Policy**
		HTTP Response Splitting	Input Validation Vulnerability	**Data Input and Output Validation**
Web Service	**Application software**	Malware	Security defects in software Insecure design Over-privileged users Over-privileged code	**Malware Protection**
		Modification of information	Insecure Communication Insecure Data Storage	**Cryptography and Encryption** **Data integrity**
		communication protocol hijacking	Insecure Communication	**Cryptography and Encryption** **Authentication and Authorisation**
		Blind SQL Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Brute Force Attack	Insufficient Session-ID Length	**Authentication and Authorisation**
		Guessing passwords	Authentication Vulnerability	**Authentication and Authorisation**
		Bypassing authentication	Authentication Vulnerability	**Authentication and Authorisation**
		Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
		Custom Special Character Injection	Input Validation Vulnerability	**Data Input and Output Validation**

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

Asset Name	Asset Sub-category		Threat Name	Vulnerabilities	Security Controls
			Function Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			HTTP Response Splitting	Input Validation Vulnerability	**Data Input and Output Validation**
			Log Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Man-in-the-middle attack	Session Management Vulnerability Insecure Communication	**Authentication and Authorisation** **Data Input and Output Validation** **Cryptography and Encryption**
			Path Traversal	Input Validation Vulnerability	**Data Input and Output Validation**
			Repudiation Attack	Access Control Vulnerability Logging and Auditing Vulnerability	**Logging, Auditing and Accountability** **Access Control** **Non-Repudiation**
			SQL Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Server-Side Includes (SSI) Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Setting Manipulation	General Logic Error Vulnerability	**Secure Coding Guideline**
			Special Element Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Unicode Encoding	Input Validation Vulnerability	**Data Input and Output Validation**
			Web Parameter Tampering	Input Validation Vulnerability	**Data Input and Output Validation**
			Embedding Null Code	Input Validation Vulnerability Improper Neutralization of Null Byte or NUL Character	**Data Input and Output Validation**
			Cryptanalysiss	Insufficient Cryptography	**Cryptography and Encryption** **Key Management**
			Forced browsing	Access Control Vulnerability	**Access Control**
			Replay attack	Lack of session management Insufficient Cryptography	**Authentication and Authorisation** **Cryptography and Encryption**
			Information or Products from an Unreliable Source	Lack of Access Control Insecure Authorisation	**Access Control** **Authentication and Authorisation**
	Software libraries		Malware	Security defects in software Insecure design Over-privileged code	**Malware Protection**
			Function Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	**System Hardening** **Logging, Auditing and Accountability** **Secure Software Update**
	Server resources	**Processing**	Malware	Security defects in software Insecure design Over-privileged code	**Malware Protection**
			Denial of Service	Input Validation Vulnerability API Abuse Lack of Intrusion detection	**Access Control** **Authentication and Authorisation** **Intrusion Detection**
			Command Injection	Input Validation Vulnerability	**Data Input and Output Validation**
			Replay attack	Lack of session management Insufficient Cryptography	**Authentication and Authorisation** **Cryptography and Encryption**
		Memory	Malware	Security defects in software Insecure design or user error	**Malware Protection**

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

Asset Name	**Asset Sub-category**		**Threat Name**	**Vulnerabilities**	**Security Controls**
				Over-privileged code	
			Denial of Service	Input Validation Vulnerability API Abuse Lack of Intrusion detection	Access Control Authentication and Authorisation Intrusion Detection
			Buffer Overflow Attack	Buffer Overflow	Code Review
		I/O	Malware	Security defects in software Insecure design	Malware Protection
			Denial of Service	Input Validation Vulnerability API Abuse Lack of Intrusion detection	Access Control Authentication and Authorisation Intrusion Detection
			Replay attack	Lack of session management Insufficient Cryptography	Authentication and Authorisation Cryptography and Encryption
		Storage	Malware	Security defects in software Insecure design Over-privileged users Over-privileged code	Malware protection
			Attacks on privacy	Insecure Data Storage Insufficient Privacy Protection	Cryptography and Encryption Authentication and Authorisation Data Anonymisation
			Modification of information	Insecure Communication Insecure Data Storage	Cryptography and Encryption Data integrity
			Data / Sensitive information leakage	Insecure Data Storage	Cryptography and Encryption Authentication and Authorisation Data Anonymisation
			Cryptanalysiss	Insufficient Cryptography	Cryptography and Encryption Cryptography and Encryption Key Management
			Theft of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing	Device Management Policy Logging, Auditing and Accountability
			Loss of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing Lack of Backup Policy	Device Management Policy Logging, Auditing and Accountability Backup Policy
			Physical attacks	Lack of Physical Hardening	Physical Protection Client Platform Security
			Network reconnaissance	Insecure communication Lack of System Hardening	Cryptography and Encryption System Hardening
			Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	System Hardening Logging, Auditing and Accountability Secure Software Update
			Natural Disaster	Lack of physical protection	Physical Protection
			Failure of system	Lack of System Monitoring	System Monitoring Incident Management Policy
Database	**Application software**		Blind SQL Injection	Input Validation Vulnerability	Data Input and Output Validation
			SQL Injection	Input Validation Vulnerability	Data Input and Output Validation
			Manipulation of Hardware or Software	Reverse Engineering Lack of Secure Update Mechanism Insecure Default Settings	System Hardening Logging, Auditing and Accountability Secure Software Update
	Server resources	**Processing**	Denial of Service	Input Validation Vulnerability Lack of Intrusion detection Database access abuse	Access Control Authentication and Authorisation Intrusion Detection
			Information or Products from an Unreliable Source	Lack of Access Control Insecure Authorisation	Access Control Authentication and Authorisation

Appendix E List of Assets, Threats, Vulnerabilities and Controls for WBAN Application

Asset Name	**Asset Sub-category**		**Threat Name**	**Vulnerabilities**	**Security Controls**
		Memory	Denial of Service	Input Validation Vulnerability Lack of Intrusion detection Database access abuse	Access Control Authentication and Authorisation Intrusion Detection
		I/O	Denial of Service	Input Validation Vulnerability Lack of Intrusion detection Database access abuse	Access Control Authentication and Authorisation Intrusion Detection
		Storage	Data / Sensitive information leakage	Insecure Data Storage Insecure communication	Cryptography and Encryption Authentication and Authorisation Data Anonymisation
			Cryptanalysiss	Insufficient Cryptography	Cryptography and Encryption Cryptography and Encryption Key Management
			Theft of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing Lack of Backup Policy	Device Management Policy Logging, Auditing and Accountability Backup Policy
			Loss of Devices, Storage Media and Documents	Lack of Device Management Lack of Auditing Lack of Backup Policy	Device Management Policy Logging, Auditing and Accountability Backup Policy
			Information or Products from an Unreliable Source	Lack of Access Control Insecure Authorisation	Access Control Authentication and Authorisation
			Physical attacks	Lack of Physical Hardening	Physical Protection Client Platform Security
			Natural Disaster	Lack of physical protection	Physical Protection
			Failure of system	Lack of System Monitoring	System Monitoring Incident Management Policy Backup Policy
Wireless communication			Communication protocol hijacking	Insecure Communication	Cryptography and Encryption Authentication and Authorisation
			Interception of information	Insecure Communication	Cryptography and Encryption
			Eavesdropping	Insecure Communication	Cryptography and Encryption
			Man-in-the-middle attack	Session Management Vulnerability Insecure Communication	Authentication and Authorisation Data Input and Output Validation Cryptography and Encryption
			Network reconnaissance	Insecure communication Lack of System Hardening	Cryptography and Encryption System Hardening
			Masquerading attack	Lack of Access Control Insecure Authorization Insufficient Cryptography	Access Control Authentication and Authorisation Cryptography and Encryption
			Network Outage	Lack of Network resource Monitoring	Intrusion Detection Incident Management Policy
			Modification of information	Insecure Communication Insecure Data Storage	Cryptography and Encryption Data integrity
			Communication protocol hijacking	Insecure Communication	Cryptography and Encryption Authentication and Authorisation
			Sniffing attack	Insecure Communication	Cryptography and Encryption

Appendix F Expert Review Questionnaire

Name:		Date:	
Email:			

Introduction

This questionnaire is part of a research study, and your participation is significant for this study. Please remember that your participation is voluntary and that you may skip over any questions that you would prefer not to answer. The identity of the participant will be kept confidential and pseudonymised. The purpose of this questionnaire is to evaluate the usability and efficacy of the enclosed data security and privacy risk management framework for WBAN based healthcare applications. The questionnaire has six different parts as follows: section 1 gathers participant information. Section 2 includes questions about the security risk analysis process followed by section 3 which contains questions about the process to evaluate the identified security risk. Sections 4 and section 5 include questions to assess the security controls identification process and evaluate the efficacy of the selected security controls. Finally, section 6 includes questions to evaluate the overall usability and efficacy of the proposed framework.

Please answer each question by checking the appropriate box and then completing the text box if required.

Appendix F Expert Review Questionnaire

Section 1: General

1. What is your experience in WBAN based or generic healthcare application development?

   Click or tap here to enter text.

2. What is your experience in developing an application (apart from WBAN) with security and privacy requirements?

   Click or tap here to enter text.

3. Which safety/security risk management processes have you experience of implementing, and could you briefly describe those experiences?

   Click or tap here to enter text.

Section 2: Security risk analysis

Security risk analysis is the first step in the proposed framework. The purpose of the questions in this section is to evaluate the tools, techniques and methods presented in the framework for identifying security risks, threats and vulnerabilities.

1. OWASP IoT 10, CVE Top 25, ENISA, BSI and OWASP Mobile Top 10 have been used as a source to identify WBAN threats and vulnerabilities for this framework. Do you know of any other sources?

☐	Yes	☐	No

   If yes, please name them

   Click or tap here to enter text.

2. The security risk analysis part of this framework recommends using threat modelling on the application system architecture to identify vulnerabilities. Do you think using threat modelling on the system architecture is the best approach?
    a. If yes, which threat modelling tool and/or which threat modelling method is most effective? Please state why.

        Click or tap here to enter text.

    b. If no, please state why and what approach you would recommend

        Click or tap here to enter text.

Section 3: Evaluate identified security risks

The security risk evaluation process helps to determine whether the risks identified in the security risk analysis step are acceptable or not. The framework recommends using the combination of 'impact' and 'likelihood' as factors in evaluating security risks.

1. Do you think that the 'impact level' and 'likelihood' factors are sufficient for security risk acceptance criteria?

□	Yes	□	No

If no, please state why. Which other factor needs should be taken into consideration?

Click or tap here to enter text.

Section 4: Identification and implementation of security controls

The ‘Identification and Implementation of Security Controls’ section of the framework provides the process for selecting security controls, along with each control’s implementation detail. The purpose of the questions in this section is to determine if:

- The framework consists of the appropriate security controls
- Whether the security controls have adequate implementation detail
- If the control selection process could be improved

1. Do you think the proposed security controls in Table Appendix E-1 under Appendix E assure data security and privacy for WBAN applications?

□	Yes	□	No

If no, which threats and vulnerabilities do they not mitigate?

Click or tap here to enter text.

2. The sources used to identify security controls and their respective implementation detail for WBAN applications are ISO/IEC 80001-2-2, NIST 800-53, ISO 27002, ISO 27799, ISO/IEC 11770, NIST 800-175B, NIST 800-56A, RFC 6749, OWASP, blog posts and research papers. Do you know of any other sources which may be relevant?

Click or tap here to enter text.

3. Are there any security controls you would remove?

□	Yes	□	No

If yes, which ones and why?

Click or tap here to enter text.

4. Appendix C of the framework presents the implementation detail for each security control. Do the security controls contain adequate implementation detail for the developer to implement the control?

□	Yes	□	No

If no:

- Which controls need more detail and what type of detail is required?

Click or tap here to enter text.

- Which controls need less detail?

Click or tap here to enter text.

5. The framework recommends using:

- Unit-testing to minimise the risk of exposure to vulnerabilities due to coding errors
- Code review to increase the efficacy of the security control during the implementation phase

Do you think both approaches are sufficient?

□	Yes	□	No

If no, please state why?

Click or tap here to enter text.

6. Do you think the security control selection process presented in Fig 9 under Appendix A is correct and sufficient for WBAN applications?

□	Yes	□	No

If no, please state why?

Click or tap here to enter text.

Section 5: Overall evaluation of security controls

Upon completion of the implementation of security risk controls, an evaluation process is required to evaluate the overall security and privacy risks of the application. The purpose of the questions in this section is to determine:

- Whether the approach is adequate to evaluate the security and privacy risk level of the application.
- Identify alternative approaches which could be used, instead of the penetration testing and/or vulnerability scanning as recommended in the framework.

1. The framework recommends the use of penetration testing and/or vulnerability scanning to evaluate the security and privacy risk level of the application. Do you think both penetration testing and/or vulnerability scanning are required for evaluating the security and privacy risk level of WBAN applications?

   a. If yes, please state why

   Click or tap here to enter text.

   b. If no, please name which one will be more applicable and why.

   Click or tap here to enter text.

2. Should any other evaluation techniques be considered?

□	Yes	□	No

If yes, which ones and why?

Click or tap here to enter text.

Section 6: Usability and Efficacy

The purpose of this section is to gather information on the usability and effectiveness of the framework.

1. Is it easy to understand and follow the proposed framework?

☐	Very easy	☐	Easy	☐	Neither	☐	Difficult	☐	Very difficult

If you answered anything other than very easy, please comment on how the framework could be made easier to understand and follow.

Click or tap here to enter text.

2. Do you think this framework has sufficient detail for a developer to use?

☐	Yes	☐	No

If no, please comment on how the framework could be made more developer friendly.

Click or tap here to enter text.

3. In your opinion how effective is the framework in assuring security and privacy of WBAN applications?

☐	Very effectiv e	☐	Effectiv e	☐	Neither effective or ineffective	☐	Ineffective	☐	Very ineffective

If you answered anything other than very effective, please comment on how the framework could be made more helpful.

Click or tap here to enter text.

4. Would you consider the proposed framework if you are planning to develop a WBAN based healthcare application?

□	Yes	□	No

If no, please state why

Click or tap here to enter text.

5. Do you have any other suggestions for how the framework could be improved?

Click or tap here to enter text.

6. Do you have any additional comments you would like to make?

Click or tap here to enter text.

Appendix G Interview Questionnaire

Name:		Date:	
Email:			

Introduction

This questionnaire is part of a research study, and your participation is significant for this study. Please remember that your participation is voluntary and that you may skip over any questions that you would prefer not to answer. The identity of the participant will be kept confidential and pseudonymised. The purpose of this questionnaire is to identify the challenges for assuring security and privacy of WBAN based healthcare applications. The questionnaire has three different parts as follows: section 1 gathers methodological challenges relate to the difficulties companies found in integrating security identification, analysis, testing and monitoring in their development methodology. Section 2 includes questions for the organisational challenges relate to company's policies, factors about market and external stakeholders. Finally, section 3 contains questions for the technical challenges relate to specific security concerns when designing and implementing WBAN applications.

Please answer each question by checking the appropriate box and then completing the text box if required.

Appendix G Interview Questionnaire

Section 1: Methodological Challenges

The purpose of the questions in this section is to identify the methodological challenges.

1. Do you face any challenges to incorporate the security and privacy requirements in your software development process?

   Click or tap here to enter text.

2. What challenges you face to prioritise the security and privacy controls without compromising the release plan?

   Click or tap here to enter text.

Section 2: Organisational Challenges

The purpose of the questions in this section is to identify the organisational challenges.

1. What are the regulatory compliances you are planning to incorporate in your application?

   Click or tap here to enter text.

2. What level of knowledge do you have for the regulatory requirements, standards and policies?

   Click or tap here to enter text.

Section 3: Technical Challenges

The purpose of the questions in this section is to identify the technical challenges.

1. Do you have comprehensive understanding of the system architecture of the application?

   Click or tap here to enter text.

2. Do you have comprehensive understanding of the data flow and respective assets for the application?

   Click or tap here to enter text.

3. Do you have any physical resource constraints devices?

☐	Yes	☐	No

   If yes, do you face any challenges to implement security and privacy mechanism?

   Click or tap here to enter text.